

Cybersecurity – Supplier’s Frequently Asked Questions

Table of Contents

Cybersecurity Compliance and Risk Assessment (CCRA):	3
1. How many questionnaires are there, and which am I required to complete?	3
2. When will LM suppliers be required to complete the CCRA?	3
3. How can we complete the CCRA if we don’t have access to Supplier Management (SM)?	3
4. What is Exostar Supplier Management (SM) and how can I get access to it?	3
5. How can a supplier improve their Cyber Rating?	4
6. How does the CCRA - Risk calculate the risk rating and how is it assessed?	5
7. I’ve completed the <i>CCRA - Compliance</i> but I am not shown as Compliant with DFARS 252.204-7012. What do I need to do to become compliant?	5
8. I’ve completed the <i>CCRA - Compliance</i> , but I am not shown as Compliant with DFARS 252.204-7019/ - 7020. What do I need to do to become compliant?	6
9. Is there a way to complete CCRA offline and then upload it to SM?	6
Cybersecurity Maturity Model Certification (CMMC) Questions	7
10. What is CMMC?	7
11. Where can I go to learn more about CMMC?	7
12. How do I know if CMMC is applicable to my organization?	7
13. When will suppliers be required to implement CMMC?	8
14. What CMMC Level are suppliers required to have?	8
15. When will suppliers need to have their CMMC Level 2 third-party (C3PAO) certifications?	9
16. What is the cost of implementing CMMC?	9
17. Are there any resources to help suppliers with preparing for CMMC?	9
General Questions:	10
18. What expertise is needed to understand how to improve my company’s cybersecurity posture.....	10
19. What resources are available to help a supplier with implementing the NIST controls?	11
20. I am a provider of consulting services and/or labor resources. Am I required to complete the CCRA?	11
21. I am a provider of consulting services and/or labor resources, is CMMC applicable to me?	12
22. We currently do not hold any contracts with Lockheed Martin; do we still have to complete the CCRA?	12
Reminder notices from Exostar and Lockheed Martin	12
23. Why do I keep receiving follow up/reminder emails from Lockheed Martin and Exostar?	12
24. I’ve already completed the questionnaires, but I am still receiving reminder notices.	13

Cybersecurity – Supplier’s Frequently Asked Questions

Replication: Form Groups.....14

- 25. We have more than one business unit as a supplier to Lockheed Martin with separate accounts in Exostar; do we have to manually complete the questionnaires for each account? 14
- 26. 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. 14

TPM related questions: 14

- 27. How do I get to the TPM portal? 14
- 28. How can I complete my annual self-certification when receiving a warning that the CCRA – Compliance is incomplete or that the CMMC/SPRS status is expired? 14

SM Related Questions: 15

- 29. How can I access and complete the CCRA on SM? 15
- 30. I don’t see Supplier Management – Lockheed Martin on my MAG dashboard..... 16
- 31. I am a returning vendor with an Expired profile and do not have access to SM to complete the CCRA – Compliance. 16
- 32. The Supplier Management – Lockheed Martin application is showing as “Pending Approval” on the MAG dashboard. Who needs to approve it? 16
- 33. What are the system requirements to access SM?..... 17
- 34. I can see the questionnaire on the SM dashboard, but how can I start responding? 17
- 35. I’ve completed the questionnaires, but my LM Buyer/Subcontract Administrator says that it is not completed on their systems. 17

Cybersecurity – Supplier’s Frequently Asked Questions

Cybersecurity Compliance and Risk Assessment (CCRA):

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

There is one questionnaire called the Cybersecurity Compliance and Risk Assessment (CCRA), but it has two parts: Compliance and Risk.

- **Cybersecurity Compliance and Risk Assessment (CCRA) - Compliance:** The CCRA – Compliance questionnaire **is required for ALL LM suppliers**. It provides questions related to the applicability and compliance status with cyber Federal Acquisition Regulations (FAR), Defense Federal Acquisition Regulation Supplement (DFARS), handling LM Sensitive Information, and Cybersecurity Maturity Model Certification (CMMC). The CCRA is implemented in a web-based format hosted on Exostar’s **Supplier Management (SM)** application.
- **Cybersecurity Compliance and Risk Assessment (CCRA) – Risk:** Suppliers that are required to implement safeguards to protect sensitive data and attest to **not having** a CMMC Level 2 status or higher (Self or C3PAO) on the *CCRA – Compliance* questionnaire will be required to complete the *CCRA – Risk*. It will be used to derive a cyber risk rating for suppliers that are:
 - Required to meet DFARS 252.204-7012 or CMMC requirements but do not have a CMMC Level 2 or higher in their response to the *CCRA – Compliance* questionnaire, **OR**
 - Not required to meet DFARS 252.204-7012 or CMMC requirements but are handling LM Sensitive Information (i.e., indirect suppliers).

2. When will LM suppliers be required to complete the CCRA?

All LM suppliers are required to complete the CCRA.

- **New Vendors** – New suppliers being onboarded will be required to complete the CCRA on Exostar's Supplier Management (SM) as part of the registration process.
- **Existing Vendors** – All existing suppliers are required to complete or resubmit their CCRA upon expiration of their Supplier Performance Risk System (SPRS) or CMMC statuses.
- **Expired Vendors reactivating their accounts** – Expired suppliers are required to complete the CCRA during the profile recertification process.

NOTE: Suppliers must complete the CCRA to **Submit Certifications and Representation** on Exostar Trading Partner Manager (TPM) self-certification page.

3. How can we complete the CCRA if we don’t have access to Supplier Management (SM)?

Instructions on how to navigate to SM to complete the CCRA can be found here:

https://www.myexostar.com/?ht_kb=tpm-cyber-security (User Guide)

4. What is Exostar Supplier Management (SM) and how can I get access to it?

Supplier Management (SM) is the application that hosts the CCRA. More information on SM can be found [here](#). Suppliers that do not have access to SM may contact Exostar Support online or by phone for assistance:

- Online: <https://www.myexostar.com/knowledge-base/contact-support/>
- Phone Support is available Monday to Friday 3:00 AM EST – 9:00 PM EST

Cybersecurity – Supplier’s Frequently Asked Questions

USA & World-Wide Phone: +1 703-793-7800

United Kingdom Phone: 0203 3007093

Australia: +61 2 8073 8383

Suppliers can access the SM application through Exostar’s Managed Access Gateway (MAG) or Trading Partner Manager (TPM).

From MAG:

The screenshot shows the Exostar MAG interface. At the top, there's a header with 'My 2FA Credentials' and a warning that a 2FA credential is required. Below this, there's a section for 'Elevate your credential strength' and a link to 'Link your existing credentials'. The main section is 'Applications', with tabs for 'My Applications', 'Open Applications', and 'Request Applications'. Under 'My Applications', there are four application cards: 'Lockheed Martin Procure to Pay Service', 'Exostar LLC ForumPass 7 - US', 'Exostar LLC Supplier Management- Lockheed Martin' (highlighted with a red box), and 'SAP NS2 PROD LMSupplier Connect'. Each card shows its status (Active), last access time, and a 'Launch' button.

From TPM:

The screenshot shows the 'Cyber Security' section of the Exostar TPM interface. It contains instructions for completing the CCA in Exostar's Supplier Management (SM) system. A red box highlights the link: 'Click here to submit or update your CCA in Exostar's Supplier Management (SM) System'. Below this, there are links for FAR 52.204-21 Applicability, DFARS 252.204-7012 (NIST) Compliance, and DFARS 252.204-7020 (SPRS) Status.

See the **Supplier Guide** provided on the [Supplier Management Training Resources](#) support page.

5. How can a supplier improve their Cyber Rating?

The Cyber Rating is derived from the two questionnaires, *CCRA – Compliance* or *CCRA - Risk*:

CCRA – Compliance

Cybersecurity – Supplier’s Frequently Asked Questions

- If the supplier’s response to question 4.0 and 4.1 of the *CCRA – Compliance* questionnaire reflects a CMMC Level 2 (Self or C3PAO) or higher status, then the supplier will receive a **Green** cyber rating.
 - CMMC statuses for a **Green** rating includes (any one): CMMC Final Level 2 (Self), CMMC Conditional Level 2 (Self), CMMC Final Level 2 (C3PAO), CMMC Conditional Level 2 (C3PAO), CMMC Final Level 3 (DIBCAC), or CMMC Conditional Level 3 (DIBCAC)
- If the supplier does not have CMMC Level 2 or higher status, they must complete the *CCRA – Risk* to obtain a cyber risk rating.

CCRA - Risk

- Cyber Rating is derived based on a subset of (31) thirty-one NIST SP 800-171 controls that are separated into 3 Categories: (11) Category 1, (10) Category 2, (10) Category 3.
- To be **Green**, suppliers must attest that all 31 of the Cyber Security Controls on the *CCRA – Risk* are implemented.

6. How does the CCRA - Risk calculate the risk rating and how is it assessed?

The Cyber Rating derived from the *CCRA – Risk* is based on a subset of (31) thirty-one NIST SP 800-171 Controls that are separated into 3 Categories: (11) Category 1, (10) Category 2, (10) Category 3.

Green Rating = (All Category 1, 2, and 3 controls are implemented)

- Negligible to minimal risks are identified based on response provided. The supplier has a strong performing cyber risk management program.

Yellow Rating = (All Category 1 implemented AND > 1 Category 2 or 3 implemented)

- Minimal to moderate risks are identified based on the response provided. The supplier has a Cyber risk management program with good protection in place, but additional risk mitigations are likely required to protect Sensitive Information and/or Government/DOD Controlled Unclassified Information (CUI).

Red Rating = (Less than 11 Category 1 implemented)

- Moderate to significant risks are identified based on the response provided. The supplier has minimal or no cyber risk management program and significant cyber protections are lacking.

7. I’ve completed the CCRA - Compliance but I am not shown as Compliant with DFARS 252.204-7012. What do I need to do to become compliant?

The supplier can attest compliance with DFARS 252.204-7012 through the *CCRA - Compliance* (questions 2.0 and 2.1) that all 110 NIST cybersecurity controls are implemented OR for controls not fully implemented, the supplier must have a documented Plan of Action and Milestone (POAM) in their System Security Plan (SSP).

Questions 2.0 and 2.1 must both be answered **Yes** to be shown as compliant with DFARS 252.204-7012 on the *CCRA*.

Response Guidance for Question 2.1

Cybersecurity – Supplier’s Frequently Asked Questions

Answer **Yes** if your organization can demonstrate that, for all **110 NIST SP 800-171 security controls**, each control has been assessed / classified as one of the following:

- **Implemented** – the control is fully in place and operational, and the implementation is described in the System Security Plan (SSP);
- **Not Applicable** – the control does not apply to the supplier’s IT environment, with a documented justification included in the SSP; or
- **Addressed in a POA&M** – the control is not yet fully implemented, but the supplier has a documented Plan of Action and Milestones (POA&M) that outlines remedial actions, timelines, and responsible parties, and the POA&M is referenced in the SSP.

In addition, your organization has a **complete System Security Plan (SSP)** document that:

- Describes how the implemented controls are satisfied.
- Contains the documented justifications for any “Not Applicable” controls; and
- Includes or references the POA&M for any controls that are not fully implemented.

Answer **No** if any of the below apply:

- You do not plan on implementing NIST SP 800-171
- You do not have a System Security Plan (SSP) that addresses how you've implemented or plan to implement NIST SP 800-171
- You do not have a POAM for NIST SP 800-171 security requirements that have not been implemented.
- You have not documented justification in your SSP for any controls treated as Not Applicable to your IT environment

Note: Part of DFARS Clause 252.204-7012 requirement to rapidly report cyber incidents is for suppliers to have or be able to obtain a DoD-approved Medium Assurance Certificate to report cyber incidents to <https://www.dc3.mil/Missions/DIB-Cybersecurity/DIB-Cybersecurity-DCISE/>. This will not be asked on the questionnaire and will not affect your compliant status on the CCRA.

8. I’ve completed the **CCRA - Compliance**, but I am not shown as **Compliant with DFARS 252.204-7019/-7020**. What do I need to do to become compliant?

The supplier can attest compliance with DFARS 252.204-7019/ -7020 through the CCRA - Compliance (questions 3.0, 3.1, and 3.2) that the supplier completed an assessment using the [NIST SP 800-171 DoD Assessment Methodology](#) and submitted the score to the DoD-managed [Supplier Performance Risk System](#).

To be compliant with DFARS 252.204-7020 on the CCRA, the following conditions must be met:

- Questions 3.0 and 3.1 must be **Yes**
- Question 3.2 must have a **valid SPRS assessment date** that is less than 3 years old.

See the linked [Quick reference guide](#) for instructions on how to submit your DoD Assessment score to SPRS.

9. Is there a way to complete **CCRA offline** and then upload it to **SM**?

SM does not currently support upload of the CCRA.

Cybersecurity – Supplier’s Frequently Asked Questions

Cybersecurity Maturity Model Certification (CMMC) Questions

10. What is CMMC?

The Cybersecurity Maturity Model Certification (CMMC) framework consists of the security requirements from NIST SP 800-171 Rev 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, and a subset of the requirements from NIST SP 800-172, Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171. The model framework organizes these practices into a set of domains, which map directly to the NIST SP 800-171 Rev 2 families. There are three levels within CMMC – Level 1, Level 2, and Level 3.

11. Where can I go to learn more about CMMC?

The Department of War (DoW) Chief Information Officer [CMMC webpage](#) is the authoritative source for CMMC program information.

The ND-ISAC CyberAssist website also provides CMMC [self-paced](#) and [live monthly training](#) sessions.

12. How do I know if CMMC is applicable to my organization?

The CMMC requirements only apply if you are/will be performing under CMMC contracts/subcontracts (DFARS 252.204-7021 dtd 10 Nov 26). If you are **not** performing on DoD contract/subcontracts, then the CMMC requirements will not apply. If the products or services you're offering meet the definition of commercially available off-the-shelf (COTS) items, as defined in [FAR 2.101](#), then you are exempt from the CMMC requirements.

If you are performing on DoD subcontracts and are/will be receiving Federal Contract Information (FCI), then CMMC Level 1 (Self) will be required. If you are/will be receiving Controlled Unclassified Information (CUI), then CMMC Level 2 (Self or C3PAO) will be the minimum security requirement.

FCI and CUI Defined

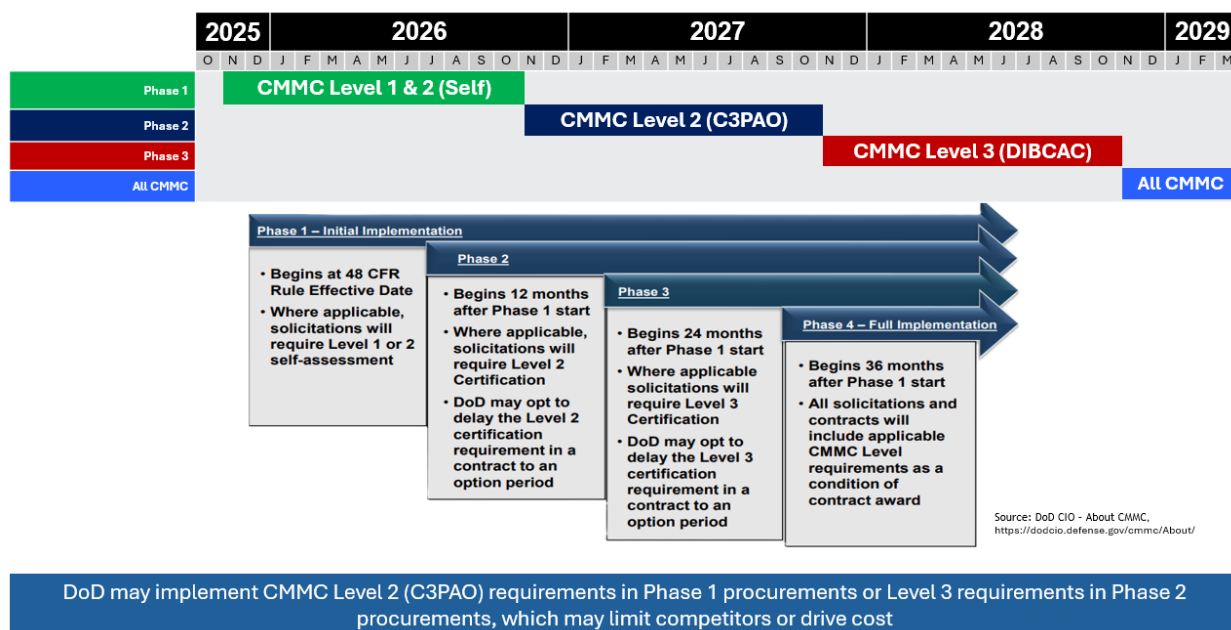
- **Federal Contract Information (FCI)**, as defined by [FAR 52.204-21](#), *Basic Safeguarding of Covered Contractor Information Systems*, means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver or service to the Government, but not including information provided by the Government to the public (such as on public websites) or simple transactional information, such as necessary to process payments. (Generally, a Lockheed Martin Purchase Order under a DoD Prime Contract will constitute Federal Contract Information, with contents such as Prime Contract Number, DPAS Rating, or other Gov't / Program Flow Down information.)
- **Controlled Unclassified Information**, as defined by 32 CFR part 170, is information (1) held or created by the U.S. government; (2) provided by the U.S. government to a non-government entity, such as Lockheed Martin and its subcontractors; or (3) created under or included in a performance requirement (i.e., a non-administrative requirement) of a contract, provided that a law, regulation, or U.S. government-wide policy require that the information be protected. CUI does not include (1) classified information, (2) information that was not created or delivered as a requirement under a contract, or (3) public information related to commercial off-the-shelf items.

Cybersecurity – Supplier’s Frequently Asked Questions

13. When will suppliers be required to implement CMMC?

Starting on November 10, 2025, new DoD contracts, extension, or mods (except those for COTS items) began requiring some level of CMMC compliance depending on the type of sensitive data being handled (i.e., FCI or CUI). DoD’s CMMC assessment requirements will be implemented using a four-phase plan over three years. The phases add CMMC Level requirements incrementally, starting on November 10, 2025, with self-assessments in Phase 1, progressing with certifications made by third-party assessors (e.g., C3PAOs and DIBCAC) in Phases 2 & 3, and ending with full implementation of program requirements in Phase 4 (Nov 10, 2028). However, in some procurements, the DoD may implement CMMC requirements in advance of the planned phase.

CMMC 2.0 Phased Approach



14. What CMMC Level are suppliers required to have?

CMMC requirements will be flown down to suppliers’ subcontracts during solicitations and/or RFx:

- If a subcontractor handles only FCI, a CMMC Level 1 (Self-Assessment) or higher is required.
- If a subcontractor handles CUI, a CMMC Level 2 (Self-Assessment) or higher is required.
- If a subcontractor handles CUI and the associated prime contract has a requirement for CMMC Level 2 (C3PAO), then the CMMC Level 2 (C3PAO) is the minimum requirement for the subcontractor.
- If a subcontractor handles CUI and the associated prime contract has a requirement for CMMC Level 3 (DIBCAC), then the CMMC Level 2 (C3PAO) is again the minimum requirement for the subcontractor. CMMC Level 3 (DIBCAC) will be required of subcontractors only as specified by the DoD prime contracting officer.
- More information on the CMMC Level determination can be found [here](#).

Contact your primary LM buyer for details on your subcontract CMMC requirements.

Prime contractors are responsible for ensuring their subcontractors have the appropriate CMMC level as a condition of the subcontract award.

Cybersecurity – Supplier’s Frequently Asked Questions

15. When will suppliers need to have their CMMC Level 2 third-party (C3PAO) certifications?

According to the DoW’s [phased implementation plan](#), Prime Contracting Officers (PCOs) will begin incorporating CMMC Third-Party Assessment Organization (C3PAO) assessment requirements in Phase II starting on November 10, 2026. Contractors may already be receiving solicitations or request for proposals (RFPs) with C3PAO requirements that will be awarded at the onset of Phase II. **The supplier must have the CMMC level required by the prime contract at the time of contract or subcontract award.**

Note: The DoW reserves the right to incorporate CMMC Final Level 2 (C3PAO) beginning with Phase 1, and CMMC Final Level 3 (DIBCAC) requirements beginning with Phase 2.

If the Prime Contract contains CMMC Final Level 2 (C3PAO) requirements, subcontractors handling Controlled Unclassified Information (CUI) under that prime contract will be required to have a CMMC Final/Conditional Level 2 (C3PAO) assessment documented in DoW’s Supplier Performance Risk System (SPRS) prior to being awarded the subcontract.

- A CMMC Final Level 2 (C3PAO) is valid for three years and must be maintained for the duration of the contract.
- A CMMC Conditional Level 2 (C3PAO) is valid for contract award, but the supplier must close out all POA&Ms within the allotted 180 days and obtain a Final Level 2 (C3PAO) certification to maintain their ability to work under that contract.
- Affirmation of compliance is required to be submitted annually to SPRS to maintain the ability to work on the contract.

16. What is the cost of implementing CMMC?

DoD cost estimates for implementing CMMC and assessment costs are provided in [Title 32 CFR Part 170 rule](#).

However, cost for assessments will vary depending on the size and scope of the assessment. As the requirements phase in, CMMC will be a cost of doing business for any defense industrial base (DIB) contractor (large, mid-size, or small). The costs of satisfying CMMC Level 1-3 requirements scale with the organization’s IT footprint and for Level 2-3, the complexity of the organization’s CUI network environment (which may be the full enterprise network, or an enclave associated with one or more specific DoD contracts). Organizations of all sizes need to assess and determine the best approach to securely managing DoD information in their IT environment. Per the regulations, businesses that do not satisfy DoD cybersecurity requirements will not be eligible for contract awards. Suppliers are encouraged to engage the [Cyber AB Marketplace](#) to get an accurate cost estimate for CMMC assessments.

17. Are there any resources to help suppliers with preparing for CMMC?

Below are resources that may help with the planning, implementing, and assessment for CMMC.

- Project Spectrum <https://www.projectspectrum.io/#/>
- NSA Cyber Security Resource Center <https://www.nsa.gov/About/Cybersecurity-Collaboration-Center/>

Cybersecurity – Supplier’s Frequently Asked Questions

- CISA Free Tools for Businesses and Services <https://www.cisa.gov/resources-tools/resources/no-cost-cybersecurity-services-and-tools>
- CISA’s Cyber Guidance for Small Businesses (extension to above) <https://www.cisa.gov/cyber-guidance-small-businesses>
- The Cybersecurity in DoD Acquisition Regulations toolbox <https://dodprocurementtoolbox.com/site-pages/cybersecurity-dod-acquisition-regulations>
- NSA’s Free PDNS (Protective Domain Name Service) available in their Cyber Collaboration Center (CCC) site <https://www.nsa.gov/About/Cybersecurity-Collaboration-Center/DIB-Cybersecurity-Services/>
- NIST’s Small Business Cybersecurity Corner <https://www.nist.gov/itl/smallbusinesscyber>
- Next-Gen Commercial Operations in Defended Enclaves (NCODE) for Small Business <https://www.army.mil/ncode>
- CMMC Resources & Documentation <https://dodcio.defense.gov/CMMC/Resources-Documentation/>
- ND-ISAC CyberAssist CMMC resources <https://ndisac.org/dibscs/cyberassist/cybersecurity-maturity-model-certification/>
- The [ND-ISAC C3PAO](#) shopping guide and [Scoring spreadsheet](#) is focused on the evaluation of C3PAOs, but can also be leveraged as considerations for selecting a cybersecurity firm (i.e., MSP, MSSP, ESP, or CSP)
- Recommend that the supplier engage a [Registered Practitioner \(RP\)](#) or [Registered Practitioner Organization \(RPOs\)](#) to assist with their CMMC implementation (including selection of a security service provider that meets the supplier needs)

General Questions:

18. What expertise is needed to understand how to improve my company’s cybersecurity posture.

Understanding and improving cyber capability levels require 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 has generally accepted industry certifications. Guidance on the 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 \(DOD\) 8140.03](#) Guided by the DoW Cyber Workforce Framework (DCWF), DoD 8140 unifies the overall DoW cyber workforce to include cyber-IT, cybersecurity, cyber effects, cyber intelligence, cyber enablers, data and artificial intelligence, and software engineering work roles under a common umbrella to better enable strategic workforce management.
 - a. focuses on the demonstration of capability, which ensures the cyber workforce is able to perform required functions in the job environment
 - b. takes a targeted, role-based approach to ensure DoW cyber workforce requirements meet both position and mission needs

Cybersecurity – Supplier’s Frequently Asked Questions

- c. was designed with flexibility in mind. It allows personnel to leverage varied development pathways, while ensuring organizations are empowered to maintain their own unique requirements based on operational demands.

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 cyber questionnaires or information on Lockheed Martin’s general supply chain cybersecurity strategy, refer to the Lockheed Martin corporate website and the suppliers link at the top right www.lockheedmartin.com/us/suppliers/cyber-security.html.

19. 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 SP 800-171 DoD Assessment Methodology](#)
- Cybersecurity Maturity Model Certification (CMMC) [Assessment Guides](#)
- DIB SCC Cyber Assist – [CMMC Resources](#)

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](#)
- An enumerated list of [CUI categories](#)
- [CUI marking handbook](#) (.pdf)
- [CFR Title 32 Vol 6 Sec 2002-20](#) (.pdf)

Other

- DoD Cyber [Incident Reporting](#) for contractors and subcontractors
- [DIBSCC CyberAssist Webpage](#) – is a repository of publicly available resources to help implement and assess cybersecurity controls.

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

All Lockheed Martin suppliers are required to complete the CCRA – Compliance survey. The CCRA – Risk will only be required when the supplier’s response to the CCRA – Compliance survey indicates that they have a safeguarding requirement to protect sensitive data but do not have a CMMC Level 2 (Self or C3PAO) or higher status.

Cybersecurity – Supplier’s Frequently Asked Questions

21. I am a provider of consulting services and/or labor resources, is CMMC applicable to me?

- If you are not performing on a DoD subcontract, then the CMMC requirements will not apply. If the products or services you're offering meet the definition of commercially available off-the-shelf (COTS) items, as defined in [FAR 2.101](#), then you are exempt from the CMMC requirements.
- If you are performing on DoD subcontracts and are receiving Federal Contract Information (FCI), then CMMC Level 1 (Self) will be required. If you receive Controlled Unclassified Information (CUI), then CMMC Level 2 (Self or C3PAO) will be the minimum security requirement.
- Either way, you will be required to complete the CCRA – Compliance survey. Please log into Exostar Supplier Management (SM) and complete the CCRA - Compliance attestation as soon as possible to avoid business disruptions for awarding subcontracts with CMMC requirements

22. We currently do not hold any contracts with Lockheed Martin; do we still have to complete the CCRA?

All Lockheed Martin suppliers are required to complete the CCRA – Compliance questionnaire to maintain an Active vendor profile in Exostar.

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

Reminder notices from Exostar and Lockheed Martin

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

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

Please use the **SM Guidance for TPM Users** guide on the following Exostar Resource webpage: https://www.myexostar.com/?ht_kb=tpm-training-resources (User Guide) with the following review steps:

Trading Partner Manager Review:

1. Log into TPM and navigate to the Self-Certification section (User Guide Step 1 -2)
2. Review and update “Cyber Security” information. (User Guide Step 3)
3. Ensure that the CCRA – Compliance Complete? Attribute is **Yes**

Cyber Security

The purpose of this section is to allow you to review the Cybersecurity Compliance Attestation (CCA) and provide Lockheed Martin with your compliance statuses against cyber regulations. Cyber risk will be assessed based on Cybersecurity Maturity Model Certification (CMMC) status(es) or prior CCRA submissions where CCA was not completed.

Instructions:

1. Complete the CCA in Exostar's Supplier Management (SM) system. The CCA must be completed before moving to Step 2.
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.

Cybersecurity Compliance

CCA/CCRA Last Completed Date: 2026-05-07

CCRA Complete?: Yes

FAR 52.204-21 Applicability: Applies

FAR 52.204-21 Applicability Description: Seller asserts that FAR 52.204-21 applies, (By so asserting, Seller acknowledges requirements to have implemented the Basic Safeguarding requirements for Federal Contract Information (FCI).)

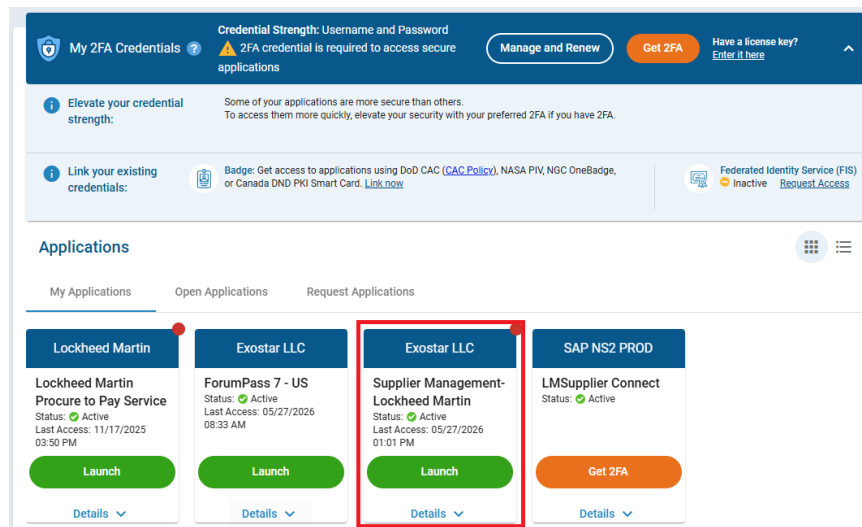
For more details on FAR 52.204-21, Basic Safeguard of Covered Contractor Information System, see <https://www.acquisition.gov/far/52.204-21>

4. If it does not say **Yes**, proceed to **Supplier Management Review**.

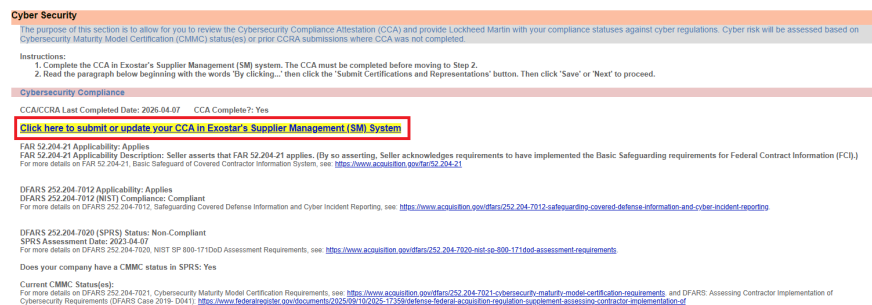
Supplier Management Review:

Cybersecurity – Supplier’s Frequently Asked Questions

1. Log into Supplier Management directly: <https://om-lmc.exostar.com/>, through the Managed Access Gateway (MAG), or Trading Partner Manager
From MAG:



From TPM:



See the **Supplier Guide** provided on the [Supplier Management Training Resources](#) support page

2. Accept **Export Control Acknowledgement**.
 3. Click on the **Pending Forms** widget and select the **CCRA - Compliance** survey
 - a. **IMPORTANT NOTE:** If the Form Request status is stuck at 20%, you can select the options menu [three dots] and **reassign** it to the user. This will increase the request status to 40% and enable form editing.
 4. Ensure that you go to the end of the questionnaire and click on the **Save** and then **Review** button to save and review the questionnaire for submission.
 5. When applicable, assign the **CCRA – Risk** to the user that will be responsible for completing it.
 6. Ensure that you click on the **Submit** button to complete the survey.
 7. Instructions on how to complete the questionnaires can be found in the **TPM SM Guide** on the following Exostar Resource webpage: https://www.myexostar.com/?ht_kb=tpm-cyber-security
24. 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 (updating SPRS and CMMC statuses). Upon receipt of reminder notices the supplier must log back into Exostar, make updates to their questionnaire, and re-submit the questionnaire to complete this requirement.

Cybersecurity – Supplier’s Frequently Asked Questions

For instructions on how to update/complete the questionnaire, please use the following Exostar Resource webpage: <https://www.myexostar.com/knowledge-base/tpm-cyber-security/#update-completed-form>.

Replication: Form Groups

25. We have more than one business unit as a supplier to Lockheed Martin with separate accounts in Exostar; do we have to manually complete the questionnaires for each account?

No, Exostar’s Form Group function has been developed to allow organizations to share the completed CCRA 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 Form Grouping.

The process for requesting Form Group is provided here: <https://www.myexostar.com/knowledge-base/supplier-management-form-grouping/>

The completed spreadsheet should be submitted to [Exostar Online Support](#).

26. 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 add the additional accounts you need to the destination account fields. Once completed, submit the new request to [Exostar Online Support](#).

To remove the account(s) from an existing form group, please contact [Exostar Online Support](#).

TPM related questions:

27. How do I get to the TPM portal?

Please use the **SM Guidance for TPM Users** guide on the following Exostar Resource webpage: https://www.myexostar.com/?ht_kb=tpm-training-resources (User Guide) or web KBA: <https://www.myexostar.com/knowledge-base/tpm-cyber-security/>

28. How can I complete my annual self-certification when receiving a warning that the CCRA – Compliance is incomplete or that the CMMC/SPRS status is expired?

All suppliers are required to maintain a current CCRA – Compliance survey to “Submit Certifications and Representations” on Exostar TPM self-certification page.

1. Ensure that the *CCRA – Compliance Complete?* attribute is **Yes**

Cybersecurity – Supplier’s Frequently Asked Questions

Cyber Security

The purpose of this section is to allow for you to review the Cybersecurity Compliance Attestation (CCA) and provide Lockheed Martin with your compliance statuses against cyber regulations. Cyber risk will be assessed based on Cybersecurity Maturity Model Certification (CMMC) status(es) or prior CCRA submissions where CCA was not completed.

Instructions:

1. Complete the CCA in Exostar's Supplier Management (SM) system. The CCA must be completed before moving to Step 2.
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.

Cybersecurity Compliance

CCA/CCRA Last Completed Date: 2026-05-07 **CCRA Complete?: Yes**

FAR 52.204-21 Applicability: Applies

FAR 52.204-21 Applicability Description: Seller asserts that FAR 52.204-21 applies. (By so asserting, Seller acknowledges requirements to have implemented the Basic Safeguarding requirements for Federal Contract Information (FCI). For more details on FAR 52.204-21, Basic Safeguard of Covered Contractor Information System, see: <https://www.acquisition.gov/far/52-204-21>

2. Ensure the SPRS status is **Compliant** or **Not Applicable**

Cybersecurity Compliance

CCA/CCRA Last Completed Date: 2026-05-07 CCA Complete?: Yes

FAR 52.204-21 Applicability: Applies

FAR 52.204-21 Applicability Description: Seller asserts that FAR 52.204-21 applies. (By so asserting, Seller acknowledges requirements to have implemented the Basic Safeguarding requirements for Federal Contract Information (FCI). For more details on FAR 52.204-21, Basic Safeguard of Covered Contractor Information System, see: <https://www.acquisition.gov/far/52-204-21>

DFARS 252.204-7012 Applicability: Applies

DFARS 252.204-7012 (NIST) Compliance: Compliant

For more details on DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, see: <https://www.acquisition.gov/dfars/252-204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting>

DFARS 252.204-7020 (SPRS) Status: Compliant

SPRS Assessment Date: 2025-06-12

For more details on DFARS 252.204-7020, NIST SP 800-171 DoD Assessment Requirements, see: <https://www.acquisition.gov/dfars/252-204-7020-nist-sp-800-171-dod-assessment-requirements>

3. Ensure that all the CMMC statuses provided are **Current**

Does your company have a CMMC status in SPRS: Yes

Current CMMC Status(es):

For more details on DFARS 252.204-7021, Cybersecurity Maturity Model Certification Requirements, see: <https://www.acquisition.gov/dfars/252-204-7021-cybersecurity-maturity-model-certification-requirements> and DFARS: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019- D041): <https://www.federalregister.gov/documents/2025/09/19/2025-17359-defense-federal-acquisition-regulation-supplement-assessing-contractor-implementation-of>

CMMC Status(es)	Last Assessment Date	Last Affirmation Date	Status
CMMC Final Level 1 (Self)	11/06/2025	11/06/2025	Current
CMMC Final Level 2 (Self)	11/06/2025	11/06/2025	Current

Future CMMC Status: Will Obtain CMMC Level 2 (C3PAO)

Future CMMC Status Date: 2026-11-10

[Generate Cyber Compliance Attestation \(CCA\) Questionnaire report.](#)

If the status provided on the self-certification is not Compliant or Current, you must [update the CCRA](#) to demonstrate compliance with the associated requirements/certifications.

SM Related Questions:

29. How can I access and complete the CCRA on SM?

Suppliers can log into Supplier Management directly: <https://om-lmc.exostar.com/>, through the Managed Access Gateway (MAG), or Trading Partner Manager

From MAG:

The screenshot shows the MAG interface. At the top, there's a section for 'My 2FA Credentials' with a warning that a 2FA credential is required for secure applications. Below this, there's a section for 'Applications' with tabs for 'My Applications', 'Open Applications', and 'Request Applications'. Under 'My Applications', there are four application cards: 'Lockheed Martin', 'Exostar LLC', 'Exostar LLC', and 'SAP NS2 PROD'. The 'Exostar LLC' card is highlighted with a red box. It shows 'Supplier Management-Lockheed Martin' with a status of 'Active' and a last access time of '05/27/2026 01:01 PM'. There are 'Launch' and 'Details' buttons for each application.

From TPM:

Cybersecurity – Supplier’s Frequently Asked Questions

Cyber Security

The purpose of this section is to allow you to review the Cybersecurity Compliance Attestation (CCA) and provide Lockheed Martin with your compliance statuses against cyber regulations. Cyber risk will be assessed based on Cybersecurity Maturity Model Certification (CMMC) status(es) or prior CCRA submissions where CCA was not completed.

Instructions:
1. Complete the CCA in Exostar's Supplier Management (SM) system. The CCA must be completed before moving to Step 2.
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.

Cybersecurity Compliance

CCA/CCRA Last Completed Date: 2026-04-07 CCA Complete?: Yes

Click here to submit or update your CCA in Exostar's Supplier Management (SM) System

FAR 52.204-21 Applicability: Applies
FAR 52.204-21 Applicability Description: Seller asserts that FAR 52.204-21 applies. (By so asserting, Seller acknowledges requirements to have implemented the Basic Safeguarding requirements for Federal Contract Information (FCI). For more details on FAR 52.204-21, Basic Safeguard of Covered Contractor Information System, see: <https://www.acquisition.gov/far/52-204-21>)

DFARS 252.204.7012 Applicability: Applies
DFARS 252.204.7012 (NIST) Compliance: Compliant
For more details on DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, see: <https://www.acquisition.gov/dfars/252-204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting>

DFARS 252.204.7020 (SPRS) Status: Non-Compliant
SPRS Assessment Date: 2023-04-07
For more details on DFARS 252.204-7020, NIST SP 800-171 DoD Assessment Requirements, see: <https://www.acquisition.gov/dfars/252-204-7020-nist-sp-800-171-dod-assessment-requirements>

Does your company have a CMMC status in SPRS: Yes

Current CMMC Status(es):
For more details on DFARS 252.204-7021, Cybersecurity Maturity Model Certification Requirements, see: <https://www.acquisition.gov/dfars/252-204-7021-cybersecurity-maturity-model-certification-requirements> and DFARS Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-10413) <https://www.federalregister.gov/documents/2020/05/17/2020-05-17-2019-10413-federal-acquisition-regulation-scientific-assessment-assessing-contractor-implementation-of>

See the **Supplier Guide** provided on the [Supplier Management Training Resources](#) support page

30. I don't see Supplier Management – Lockheed Martin on my MAG dashboard

Suppliers that do not have access to SM may request access to the application from Managed Access Gateway (MAG) administrator console or contact Exostar Support online or by phone for assistance:

Request Access through MAG, see: <https://www.myexostar.com/knowledge-base/mag-organization-administrator/#manage-application-access>

Contact Exostar Customer Support

- Online: <https://www.myexostar.com/knowledge-base/contact-support/>
- Phone Support is available Monday to Friday 3:00 AM EST – 9:00 PM EST

USA & World-Wide Phone: +1 703-793-7800

United Kingdom Phone: 0203 3007093

Australia: +61 2 8073 8383

31. I am a returning vendor with an Expired profile and do not have access to SM to complete the CCRA – Compliance.

Suppliers that do not have access to SM may contact Exostar Support online or by phone for assistance:

- Online: <https://www.myexostar.com/knowledge-base/contact-support/>
- Phone Support is available Monday to Friday 3:00 AM EST – 9:00 PM EST

USA & World-Wide Phone: +1 703-793-7800

United Kingdom Phone: 0203 3007093

Australia: +61 2 8073 8383

32. The Supplier Management – Lockheed Martin application is showing as “Pending Approval” on the MAG dashboard. Who needs to approve it?

If your application access is stuck in an “Pending Approval” state, the **Organization** or **Application Administrator** can follow the below steps to approve your access.

1. Log into the MAG dashboard via <https://portal.exostar.com>
2. Navigate to **Registration Requests** from the top tabs
3. Select **Authorize Application**
4. Click on **Click here to move to that workflow in a new browser tab/window**, if not done automatically.

Cybersecurity – Supplier’s Frequently Asked Questions

- Find the User Id associated with the desired requests and **Approve** it.
- Once approved, it may take up to 45 minutes for the system to provision access to SM. You should see a green **Launch** button on the **Supplier Management – Lockheed Martin** tile in MAG.

33. What are the system requirements to access SM?

Exostar recommends using a Microsoft Windows (10 or later) device running the latest version of Google Chrome to access SM

34. I can see the questionnaire on the SM dashboard, but how can I start responding?

To complete the questionnaire, you must **assign** the questionnaire to the appropriate personnel responsible for completing it. If the CCRA form is shown as 20% provisioned, use the 3-dot option menu to select **Reassign** it to the appropriate user. This should change the provision status to 40% and make the form accessible.

Note: Users may have multiple Exostar accounts/user IDs. Ensure that you are logged into the correct user ID for the account that the CCRA is assigned to.

Please use the **Supplier Guide** from the [Supplier Management Training Resources](#) page for detailed instructions on how to assign the CCRA.

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

Ensure that you have clicked on the **Save** and then the **Review** button at the end of the questionnaire. The review module will appear and allow you to **Submit** the CCRA, once the risk form has been assigned (when needed). This will submit the questionnaire for scoring and push updates to integrated systems.

Please use the **Supplier Guide** from the [Supplier Management Training Resources](#) page for detailed instructions on how to complete the CCRA

Screenshot of the **Save** and **Review** button located only at the end of each questionnaire:

CCRA - Compliance

Cybersecurity Compliance

Submitter

Vendor Name

Vendor Primary POC Name

Vendor Primary POC Email

Vendor IT Security POC Name

Vendor IT Security Email

Vendor Local DUNS Number(s)

Vendor CAGE Code(s)

IT

Vendor IT Security Email

IT@vendor.com

Vendor Local DUNS Number(s)

123456789

Vendor CAGE Code(s)

12345

Vendor IT Security Email - IT Security POC email address

Vendor Local DUNS Number(s) - Should accept the 9-digit numeric characters. If DUNS is more than one, use a comma and a space to separate values (i.e., 007505491, 000665432)

Vendor CAGE Code(s)/NCAGE Code(s) - CAGE Code is a five (5) position code. The format of the code is the first and fifth position must be numeric. The second, third and fourth may be any mixture of alphanumeric excluding alpha letters I and O. NCAGE code is a five (5) position code. The format of the code is all positions are alpha numeric including alpha letters I and O. If CAGE Code is more than one, use a comma and a space to separate the 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.

If you are not performing on a U.S. Government Contract and do not have a CAGE/NCAGE code, use "12345" for the purpose of this submission.

Legend information

Valid Response

Invalid Response

Disabled/Non-editable Response

Mandatory question to be answered

Exit

Previous

Save

Review

Screenshot of the **Submit** button on the Review Module.

Cybersecurity – Supplier’s Frequently Asked Questions

CCRA - Compliance

Scores

Compliance

Compliance with DFARS 252.204-7012 : Compliant
Compliance with DFARS 252.204-7020 : Compliant

CMMC_States

CMMC_States	Last_Assessment_Date	Last_Affirmation_Date	Status
CMMC Final Level 1 (Self)	2025-06-08	2026-05-27	Current

Risk

Cyber Risk Rating : Pending CCRA - Risk

CCRA - Risk Form Assignment REQUIRED

Based on your responses, a Risk Assessment is required. Please assign this form to a user who will complete it.

Assign To *

LTester MAIN634

Close

Submit