Supplier Cybersecurity Readiness Webinar

Small Business-Focused Cybersecurity Webinar: Complying with DFARS 252.204-7020 (NIST Assessment) and Preparing for CMMC

March 11, 2021
Disclaimer

• Webinar content is based on:
  o Insights and information from the Small Business Administration
  o Office of Under Secretary of Defense (OUSD) CMMC Info
  o National Institute of Standards & Technologies (NIST) publications
  o Defense Industrial Base Sector Coordinating Council (DIB SCC) Supply Chain Task Force - CyberAssist
  o Exostar assessment documentation preparation presentation

• Lockheed Martin does not take responsibility for suppliers’ certification by the CMMC 3rd Party Assessment Organization (C3PAO)
Learning Objectives

• Demonstrate how DFARS 252.204-7020 compliance is an initial building block towards long-term CMMC requirements

• Awareness of the path towards CMMC readiness, using Cloud services, highlighting pros, cons, and advantages of watch items

• Clarify Lockheed Martin’s expectations for suppliers

• Highlight small business resources

• Address Frequently Asked Questions from small business suppliers
“DoD is taking a crawl, walk, run to implementation so companies are not put immediately at risk.” There are steps the Defense Industrial Base (DIB) must take without delay.

The first one is the “crawl.” Under a trust-but-verify model, contractors must login to the DoD’s Supplier Performance Risk System and self-report on how their companies are implementing a National Institute of Standards and Technology (NIST) requirement governing Controlled Unclassified Information (CUI).

Katie Arrington
Chief information security officer for acquisition in the Office of the Under Secretary of Defense for Acquisition and Sustainment

Source: https://breakingdefense.com/2020/12/start-of-a-new-day-dods-new-cybersecurity-regs-take-effect-today
Background of DFARS 252.204-7019/7020

The *interim rule* took effect 30 Nov 2020 / DoD implementing a 5-year phased roll-out

### DFARS Provision 252.204-7019
Notice of NIST SP 800-171 DoD Assessment Requirements

- **Solicitation Notice:** Basic Assessment Score required in SPRS for contract award
  - A [NIST SP 800-171 DoD Assessment](https://www.sprs.csd.disa.mil/default.htm) (Basic, Medium, High) summary level score must be posted into DoD’s Suppliers Risk Performance System (SPRS) for the applicable CAGE code and Systems Security Plan
  - The summary level score must remain current (not older than 3 years unless a lesser time is specified) throughout the life of the contract, task or delivery order

### DFARS Clause 252.204-7020
NIST SP 800-171 DoD Assessment Requirements

- Basic Assessment Score required in SPRS to be considered for contract award
  - Applicable to companies subject to DFARS clause 252.204-7012
  - Post award, if DoD deems a Medium or High assessment is necessary due to program sensitivity, provide DoD access to facilities, systems and personnel
  - Include clause in all subcontracts or other contractual instruments including subcontracts for commercial items
  - Confirm subcontractor compliance with SPRS reporting if receiving CUI

### DFARS Clause 252.204-7021
Cybersecurity Maturity Model Certification Requirements

- Cybersecurity Maturity Model Certification Required by contract award effective 1 Oct 2025
  - Until 1 Oct 2025, OUSD(A&S) must approve clause in new acquisitions
  - Contractor certification level must be maintained for contract duration
  - Clause must be flowed down; primes must ensure subs are certified at required CMMC level prior to awarding subcontract
  - Interim rule clauses are applicable to contracts, task orders and delivery orders
  - Not applicable to micro-purchases or solicitations exclusively for the purchase of COTS products

---

CMMC assessments and certifications required for the applicable enterprise network or network segment where FCI or CUI will be processed, stored, or transmitted in performance of the contract

Source: [https://www.sprs.csd.disa.mil/default.htm](https://www.sprs.csd.disa.mil/default.htm)
Cybersecurity Maturity Model Certification Overview

- **What is CMMC?**
  - New DoD cybersecurity framework to verify the cybersecurity posture of the Defense Industrial Base (DIB)

- **Certification conducted by Certified 3rd Party Assessment Organizations (C3PAO)**

- **Acquisition Go/No-Go Decisions**

- **Supply Chain Flow Down**
  - Mandatory flow down of CMMC requirements and verify supplier certification level

- **Official CMMC document source**

Source: [https://www.acq.osd.mil/cmmc/draft.html](https://www.acq.osd.mil/cmmc/draft.html)
Maturity Level 3 – Not just a Checklist

• Demonstrate CMMC compliance with effective Policies and Documentation:
  o Define your organization’s response to cyber incidents
  o Develop processes and procedures
    • e.g. CM.3.067: Define, document, approve, and enforce physical and logical access restrictions
  o Outline and clarify procedures for all stakeholders
  o Proper documentation serves as proof of your cybersecurity readiness

• Assessors might want to see:
  o Scan results, log files, command media, actual training programs (phishing email tests etc.), physical access restrictions, etc.

• CyberAssist (CMMC help website)
  o CMMC Level 1 Assessment Guide
  o CMMC Level 2 & Level 3 Assessment Guide

• CMMC Accreditation Body

• Documentation and Policy Requirements

Source: https://landing.exostar.com/webinar-cmmc-documentation-and-policy-requirements
CLOUD COMPUTING GUIDANCE

DFARS PROVIDES THREE DIFFERENT CASES THAT APPLY

- System Operated on Behalf of the DoD
- DoD Owned or Operated Information System
- Contractor’s Internal Cloud

NIST SP 800-171

DFARS Clause 252.204-7012
Safeguarding Covered Defense Information and Cyber Incident Reporting

CLOUD COMPUTING GUIDANCE CONT.

• Determine which cloud service providers are certified for your data and if their compliance offers are suitable for you.
  o CUI & CDI hosted with a Cloud Service Provider (CSP)

• Ensure multifactor authentication (MFA) is implemented
  o NIST Digital Identity Guidelines

• Follow The Federal Risk and Authorization Management Program (FedRAMP)
  o Consult the FedRAMP Marketplace to help identify which service providers have received their authorization.

• Examples of Compliance Resources
  o Amazon Web Services – Compliance FAQs
  o Microsoft Azure – Microsoft Compliance Offerings

• Additional Cloud Computing FAQs on Cyber Assist

Cloud Vendor Contract Checklist

✓ What cybersecurity framework(s) the vendor utilizes
✓ Background checks of vendor personnel are in place
✓ Regular vendor personnel cybersecurity training
✓ Regular review of cybersecurity artifacts provided by vendor (audits, 3rd party penetration test reports)
✓ Vendor disclosure of open source software used
✓ Establish vendor cybersecurity POCs and processes ahead of incidents
✓ Limitation of vendor access to systems and data to only those necessary for performance of the scope of work
✓ Limitation of vendor data collection to scope of work
✓ Review service limitations with enterprise user base

Your cloud implementation is only a part of the "covered systems" you need to manage
Lockheed Martin’s Expectations

• Continue to progress your NIST 800-171 implementation... Full implementation (closing all POAMs) is foundational to Cybersecurity Maturity Model Certification (CMMC) Readiness
  o Accurately maintain your vendor profile in Exostar TPM (applicability of cyber DFARS requirements)
  o Perform and regularly update your NIST 800-171 self assessment
    ▪ Leverage the Exostar questionnaire in PIM to document and share your progress
    ▪ Document your self assessment result in DoD’s SPRS using the DIBCAC assessment methodology (Exostar developing tools to translate your PIM self assessment to the required SPRS format)
  o Monitor subcontracts and PO terms and ensure flow down of all mandatory clauses to your suppliers when applicable
    ▪ Cyber DFARS 252.204-7012 / 252.204-7020

• Communicate progress to Lockheed Martin via status updates on our Survey
  o Responses to the survey ensure LM buyers know you are compliant (potential business impact)
  o Expand cyber maturity focus to prepare for CMMC Level 3
    ▪ Implement additional 20 CMMC Level 2/3 practices
    ▪ Implement CMMC Level 2/3 maturity processes

Take action to avoid disruption to new contract awards
The SBA works to ignite change and spark action so small businesses can confidently

START • GROW • EXPAND • RECOVER
The SBA Resource Partner Network

Access the right tools at the right time—wherever you are.

Approved and funded by the SBA

1,400+ partner offices nationwide

Find local resource partners near you at SBA.gov/local-assistance
Build Capacity as Your Business Develops

GROW • EXPAND
Are You Ready to Consider Federal Contracting?

The world’s largest customer, buying all kinds of products & services

Required by law to provide contract opportunities to small businesses

Evaluate your readiness & learn more by visiting SBA.gov/contracting
Qualify for Federal Contracts with Certifications

The SBA works with federal agencies to award at least 23% of all prime government contracting dollars each year to small businesses that are certified with the **SBA’s contracting programs**. Programs include:

| 8(a) Business Development Program | Historically Underutilized Business Zones (HUBZone) Program | Women-Owned Small Business (WOSB) Program | Service-Disabled Veteran-Owned Program |

Learn more and determine your eligibility at [certify.SBA.gov](http://certify.SBA.gov)
All Small Mentor Protégé Program

Gain valuable business development insight from mentors who are experience government contractors. Mentors can help you:

• **Strategize** contracting & partnership opportunities

• **Navigate** the bidding and acquisition process

• **Manage** contracts by securing the appropriate business and financial systems, resources, and financial assistance
Need Access to Capital? The SBA Can Help
How Can an SBA-backed Loan Help You?

- Launch, grow, or repair a start-up
- Start or purchase a small business
- Access revolving credit or working capital for day-to-day expenses

- Purchase, renovate, or expand facilities
- Purchase inventory, equipment, or machinery
- Purchase land or real estate
- Export a product or service
Lender Match

1. Describe Your Needs
2. Interested Lenders Reply Within 2 Days
3. Talk to Lenders
4. Apply for a Loan

Find an SBA-approved lender that’s right for you by visiting

SBA.gov/lendermatch
Need to be Bonded to Bid on a Contract?

The **SBA Surety Bond Program** guarantees surety bonds from select providers so more small businesses can qualify for and win work.
Triumph Over Adversity

RECOVER
SBA Disaster Assistance Loans

Each year, the SBA provides billions of dollars in low-interest, long-term disaster loans to help small businesses, homeowners, and renters recover from declared disasters. Loans may cover:

- Real Estate
- Personal Property
- Economic Injury
- Machinery & Equipment
- Inventory
- Active Duty Military
SBA Cyber Security Resources
Planning and assessment tools

There’s no substitute for dedicated IT support—whether an employee or external consultant—but businesses of more limited means can still take measures to improve their cybersecurity.

• **FCC Planning Tool**
  The Federal Communications Commission offers a [cybersecurity planning tool](#) to help you build a strategy based on your unique business needs.

• **Cyber Resilience Review**
  The Department of Homeland Security’s (DHS) [Cyber Resilience Review (CRR)](#) is a non-technical assessment to evaluate operational resilience and cybersecurity practices. You can either do the assessment yourself, or [request a facilitated assessment](#) by DHS cybersecurity professionals.

• **Cyber Hygiene Vulnerability Scanning**
  DHS also offers free [cyber hygiene vulnerability scanning](#) for small businesses. This service can help secure your internet-facing systems from weak configuration and known vulnerabilities. You will receive a weekly report for your action.
Cybersecurity best practices

Train your employees

- Employees and emails are a leading cause of data breaches for small businesses because they are a direct path into your systems. Training employees on basic internet best practices can go a long way in preventing cyber attacks. The Department of Homeland Security’s “Stop.Think.Connect” campaign offers training and other materials.
  - Training topics to cover include:
    - Spotting a phishing email
    - Using good browsing practices
    - Avoiding suspicious downloads
    - Creating strong passwords
    - Protecting sensitive customer and vendor information
Training and events

• **SBA training**
  - SBA 7j Training (please contact your local SBA office)
  - SBA and its resource partners host in-person and virtual events regularly.
  - Check out [upcoming cybersecurity events](#) hosted by SBA and our Resource Partners.

• **Other training**
  - The [National Cybersecurity Alliance](#), a public-private partnership, provides [virtual and in-person cybersecurity events](#) to help small business owners stay secure.
Additional Cybersecurity Resources

- Key CMMC and CUI Information Sources
  - Official CMMC document source
  - Official CMMC Updates
  - Official CMMC FAQ
  - Exostar blog entry on CMMC
  - Cyber Assist (CMMC help website)
  - CMMC Accreditation Body
  - CMMC For Suppliers
  - CMMC Vs. NIST 800-171 and other Frameworks
  - CUI Categories
  - CUI Training from National Archives
  - CUI Marking Handbook from National Archives
  - NIST HB 162 - Self-Assessment Handbook For Assessing NIST SP 800-171

- SPRS
  - Hotline #: 1-207-438-1690
  - DCMA general mailbox: dcma.lee.hq.mbx.dibcacscheduling-inbox@mail.mil
Questions & Answers