GA Supplier Day 2024

Cybersecurity

The views expressed by the presenter are solely the views of the presenter and do not necessarily reflect the views of General Atomics. General Atomics is not providing contractual direction and does not guarantee the accuracy of the data in this presentation and accepts no responsibility for any financial or other consequences arising from the use of such information. Any opinions or conclusions provided shall not be ascribed to General Atomics.

GENERAL ATOMICS

Cybersecurity

Agenda

- Introductions
- Compliance with Regulation
- CMMC 2.0
- Supplier Resources
- Questions

GENERAL ATOMICS

Introductions

Welcome to General Atomics (GA) Supplier Day 2024.

The session presenters are Kevin Pyle and Sydney LaCroix.

This session is moderated by Kylee Lockwood.

A short question and answer period will follow the presentation.

GENERAL ATOMICS

Introductions (cont.)

Kevin Pyle has been with General Atomics for 5 years. Starting as a compliance specialist, he focused on understanding government regulations and internal GA policies and procedures. Shortly after he started, he began to focus into Cybersecurity regulations, how cyber threats impact the defense industry and how we can help to better secure our infrastructure to protect against these threats in the midst of this cyber threat evolution. He serves as a GA's cybersecurity for Suppliers subject matter expert; and currently supports Process Excellence where he helps to architect and implement best in class process.

GENERAL ATOMICS

Introductions (cont.)

Sydney LaCroix has been with General Atomics (GA) for seven years. She began her time at GA as a Business Systems Analyst intern in the Facilities department while she finalized her Computer Information Assurance degree at Cal Poly Pomona. Eventually, she transitioned to the GA-ITS department with a focus on Cybersecurity compliance, end-user awareness and training, and risk management. A large part of her role is ensuring that the Company stays secure and compliant, while fostering a strong cybersecurity and risk-aware culture!

GENERAL ATOMICS

Cybersecurity

Session Overview

GENERAL ATOMICS

Cybersecurity

Session Overview

In this session, we will explore the evolution of cybersecurity, where we are today and what is coming. Cybersecurity is ever evolving is it is important that we remain vigilant in our understanding of the policies and procedures in place to ensure the safety and protection of our technical information.

Cybersecurity

Cybersecurity Evolution

GENERAL ATOMICS

Cybersecurity

What is Cybersecurity?

Cybersecurity is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.

Confidentiality
Integrity
Availability

GENERAL ATOMICS

Cybersecurity

DoD Cybersecurity Evolution

GENERAL ATOMICS

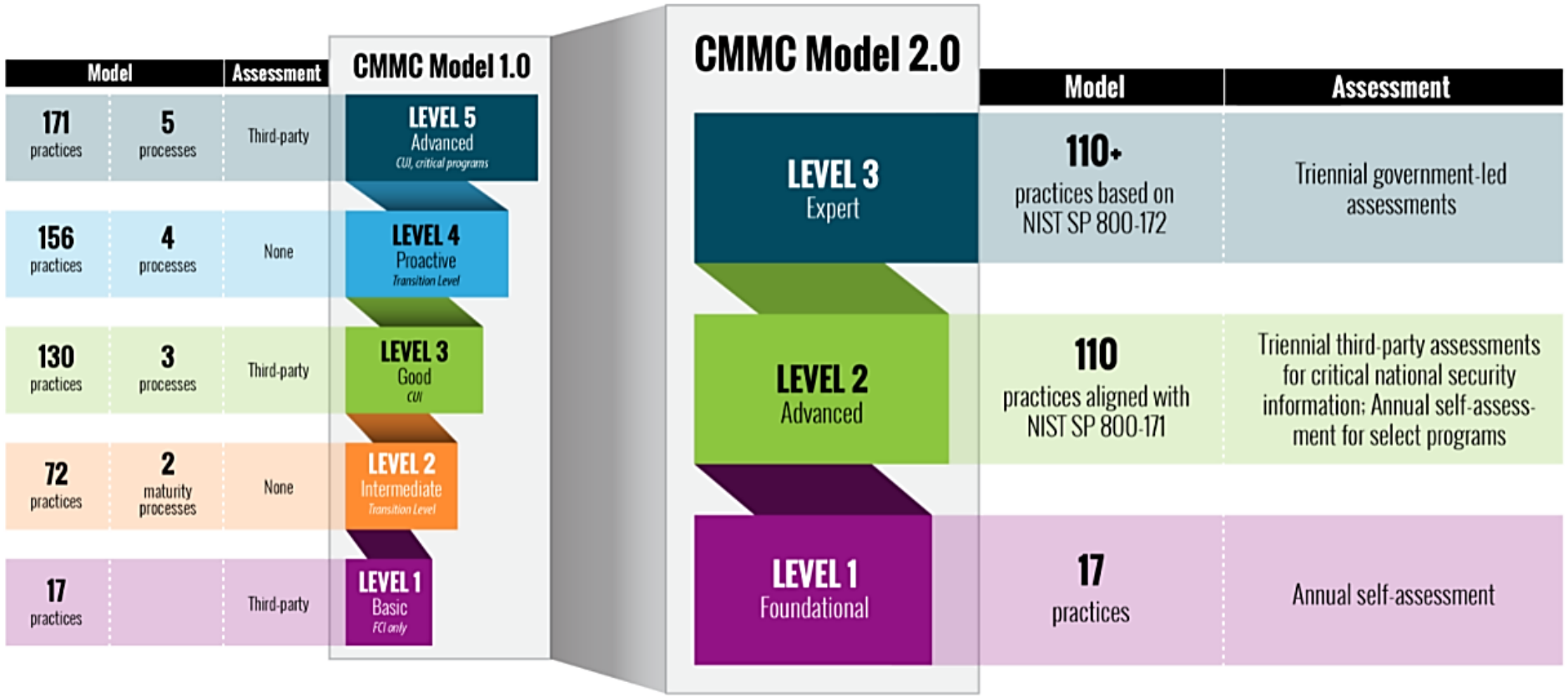
Cybersecurity

- The standards today are preparing us for the CMMC.
  - Federal Acquisition Regulation (FAR) 52.204-21 "Basic Safeguarding of Covered Contract Information Systems"
    - Mandatory flowdown in contracts, 15 basic security controls
  - Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012 "Safeguarding Covered Defense Information and Cyber Incident Reporting"
    - Self attestation of System Security Plan outlining the implementation of NIST SP 800-171 Rev. 2
  - DFARS 252.204-7020 "NIST SP 800-171 DoD Assessment Requirements"
    - Contractors' self report their score based on the NIST SP 800-171 requirements
  - DFARS 252.204-7021 "Cybersecurity Maturity Model Certification Requirements"
    - Contractors will be audited in accordance with CMMC requirements

GENERAL ATOMICS

Cybersecurity

Cybersecurity Maturity Model Certification (CMMC)

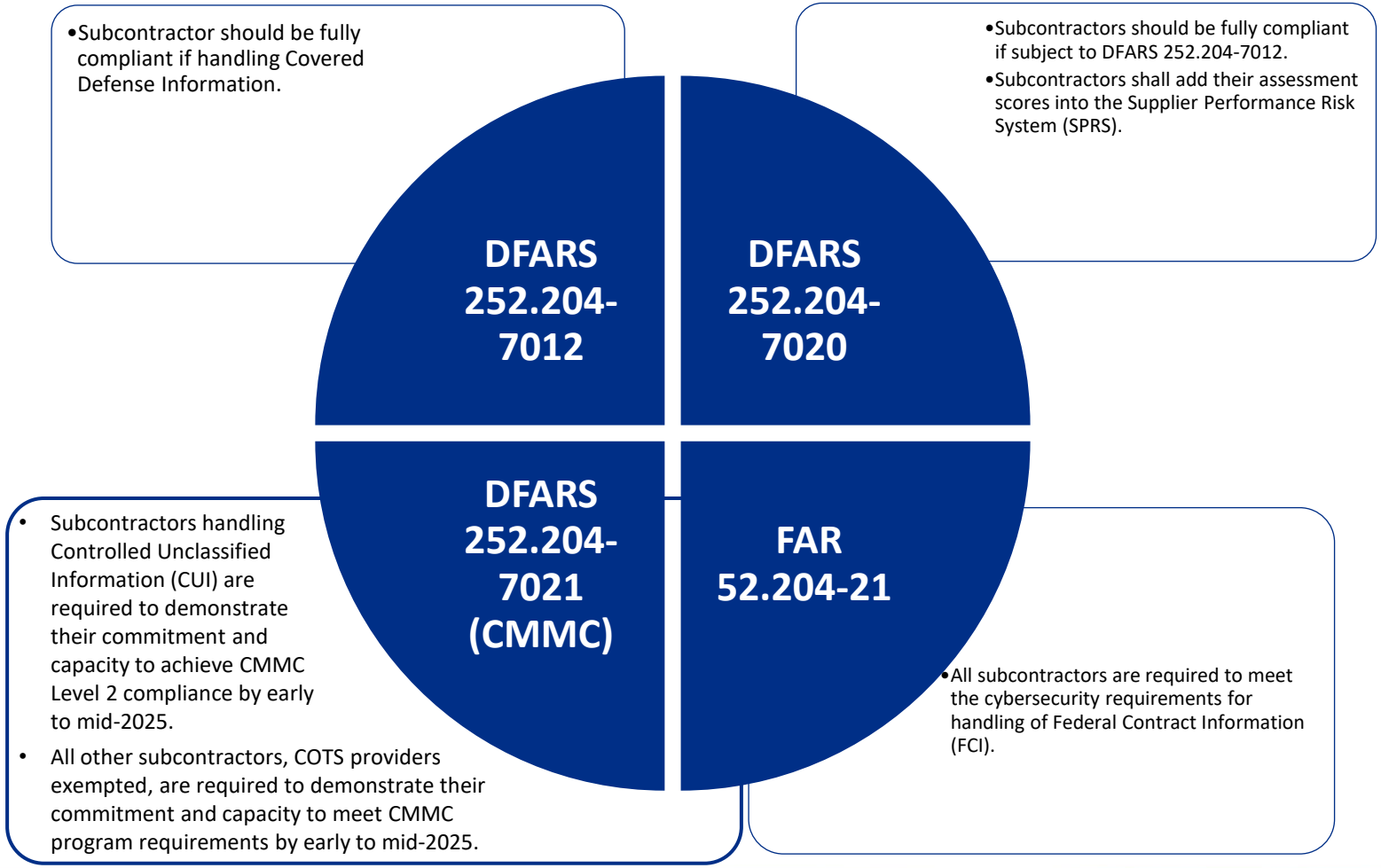


GENERAL ATOMICS

Cybersecurity

Expectations

Initiating a new supplier relationship with a supplier that will be subject to, but cannot demonstrate their ***ability and intent*** to achieve compliance with CMMC, represents an unacceptable risk to General Atomics and its contractual obligations to its customers.



GENERAL ATOMICS

How can IT organizations prepare for CMMC?

System Security Plan! (SSP)

This is worth 110 points in NIST 800-171A Scoring Methodology

Consider a CMMC RPO Assessment

A Registered Provider Organization (RPO) readiness assessment can help prepare for CMMC

Multi-factor Authentication (MFA)

Ensure some form of MFA is enabled for network access and for privileged accounts

Leverage NIST 800-171A

The NIST 800-171A Assessment Methodology is a great starting point for a self-assessment and identifying potential gaps

Review the CMMC Assessment Procedures (CAP)

This can help shed light on the types of evidence needed for each requirement

Data Flow & Assessment Boundary

Document and know how your CUI flows in and out of your environment, and include in a diagram of your assessment boundary

Encryption

Ensure proper encryption of CUI, using FIPS 140-2 validated modules, to protect data at rest and in transit

Engage the Business!

Make sure your business partners are aware of the requirements, especially those that fall outside of IT

GENERAL ATOMICS

Cybersecurity

Supplier Resources

GENERAL ATOMICS

Cybersecurity

Supplier Expectations

- **Supplier Code of Conduct**

  Cybersecurity**:** Suppliers will respond vigilantly to the growing threat of cyber warfare and will proactively secure virtual and physical hardware according to industry best practice and regulation; while reporting and mitigating any compromise of systems or information in accordance with contract terms.

GENERAL ATOMICS

Cybersecurity

Supplier Resources

IDENTIFY FCI, CUI and CDI

Proper identification and handling of FCI, CUI and CDI is a critical component of any Cybersecurity program. Federal regulations mandate specific security controls based upon the type of information a Supplier possesses or creates. FCI, CUI and CDI may be provided to Suppliers as a requirement of order performance, or it may be created by the Supplier. In either case, Suppliers must ensure that that information retains its identification and that markings are applied to derivatives. The definitions for FCI, CUI and CDI are found in their respective regulations.

CUI and CDI require a higher standard of protection and care than FCI.

GENERAL ATOMICS

Cybersecurity

Supplier Resources

PROTECT Information

GA Suppliers must take measures to protect information provided by, or created on behalf of, GA. This means applying adequate security for all 'Covered Contractor Information Systems,' or information systems that process, store, or transmit FCI, CUI or CDI.

Adequate security means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information. These measures are outlined in FAR 52.204-21 and DFARS 252.204-7012 and are derived from National Institute of Standards and Technology (NIST) Special Publication (SP) SP 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations". To facilitate the road to compliance, NIST offers a free System Security Plan (SSP) template.

Suppliers subject to DFARS 252-204-7020 must conduct or undergo a Cybersecurity assessment in accordance with the NIST SP 800-171 DoD Assessment Methodology. Suppliers must verify that the score of their completed assessment is posted to the Supplier Performance Risk System (SPRS) prior to receiving awards containing this clause.

When these clauses apply to GA solicitations or Orders, GA will seek confirmation of your compliance with these requirements using SAP Ariba® and/or other appropriate methods.

The DIB Sector Coordinating Council (SCC) has established the DIB SCC CyberAssist website to provide trusted resources to support DIB companies and Suppliers of varying sizes with the implementation of cyber protections, improve awareness of cyber risks, regulations, and supply chain accountability.

GENERAL ATOMICS

Cybersecurity

Supplier Resources

REPORT Cybersecurity Incidents

GA Suppliers, in accordance with their contractual commitments, should notify their Purchasing Representative within 72 hours if they experience a Cybersecurity incident. Suppliers subject to DFARS 252.204-7012 must report Cybersecurity incidents to the DIBNet Portal within 72 hours of discovery. Note that a Medium Assurance Certificate is required. DoD will assign an incident number which must be provided to GA. Suppliers must abide by instructions provided by the DoD or GA, when applicable; and preserve and protect images of affected systems and data. All information related to, or suspected to be related to, the incident should be preserved in the event further analysis, or access, is requested by the DoD.

GENERAL ATOMICS

Cybersecurity

Supplier Resources

Preparing for the Cybersecurity Maturity Model Certification (CMMC)

Is your company ready for the CMMC?

The Department of Defense (DoD) Chief Information Officer (CIO) recognizes that security is foundational to acquisition, on par with cost, schedule, and performance. The DoD is committed to working with the DIB to enhance the protection of controlled unclassified information (CUI) within the supply chain.

On August 15, 2024, the DoD published the proposed rule amending 48 CFR Parts 204, 212, 217 and 252, providing guidance to contracting officers and implementing the contractual requirements related to the Cybersecurity Maturity Model Certification (CMMC) 2.0 program. CMMC 2.0 provides a framework for assessing contractor implementation of cybersecurity requirements and enhancing the protection of unclassified information within the DoD supply chain.

Proposed changes to the existing Defense Federal Acquisition Regulation Supplement (DFARS) include:

1. add references to the CMMC 2.0 program requirements proposed at 32 CFR part 170 to DFARS 252.204-7021;
2. add definitions for controlled unclassified information (CUI) and DoD unique identifier (DOD UID) to the subpart to DFARS 252.204-7021;
3. establish a solicitation provision (252.204-7YYY) and prescription; and
4. revise the existing clause language (252.204-7021) and prescription.

The proposed rule's revisions to DFARS 252.204-7021, "Cybersecurity Maturity Model Certification Requirements", create additional requirements for contractors and subcontractors including:

- Obtain a CMMC certificate from a CMMC Third-Party Assessment Organization (C3PAO) or a CMMC self-assessment for each contractor information system that will process, store, or transmit FCI or CUI prior to award and throughout performance of the contract
- Complete and maintain annually, or when a change to compliance status occurs, in SPRS an affirmation by an Affirming Official of continuous compliance with the security requirements at 32 CFR part 170 for each of the information systems that will process, store, or transmit FCI or CUI during the performance of the contract
- Notify the Contracting Officer within 72 hours when there are any lapses in information security or changes in the status of CMMC certificate or self-assessment during performance of the contract
- Confirm Subcontractors complete and maintain on an annual basis or when changes occur in status, an affirmation of continuous compliance with the security requirements associated with the CMMC level required for the subcontract

GENERAL ATOMICS

Cybersecurity

Thank you

Questions?

GENERAL ATOMICS