GA Supplier Day 2022

Cybersecurity Corner Breakout Session

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
  - Powerful Partnerships
  - Compliance with Regulations
  - CMMC 2.0
  - Supplier Resources
  - Q&A

Introductions

- Presenters
  - **Will Cannon**, Director of Business Operations, Contracts, Procurement and Proposals Management
  - **Sydney LaCroix**, Cybersecurity Risk and Compliance Manager, Information Technology Services
  - **Kevin Pyle**, Project Coordinator, Contracts, Procurement and Proposals Management
- Note Taker
  - **Jayla Peterson**, Department Administrator, Contracts, Procurement and Proposals Management
- Facilitator
  - **Will Cannon**, Director of Business Operations, Contracts, Procurement and Proposals Management

Cybersecurity

Powerful Partnerships

GENERAL ATOMICS

Powerful Partnerships

Powerful Partnerships are built upon mutual trust. We trust that GA Suppliers will take all appropriate measures to combat the growing threat of cyberattack; and will implement the controls and processes necessary to safeguard information under their control while reporting and mitigating any compromise of systems or information in accordance with contract terms and industry best practices. Together we can maintain secure environments for our nation's most critical advantage: **information**.

Cybersecurity Evolution

What is Cybersecurity?

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

Confidentiality
Integrity
Availability

DoD Cybersecurity Evolution

FAR 52.204-21
Basic Safeguarding of Covered Contractor Information Systems

Flowdown

2016

2018

Self-Attestation

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

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

Self-Reporting

2020

2023?

Certification

CMMC

Cybersecurity: Network Security

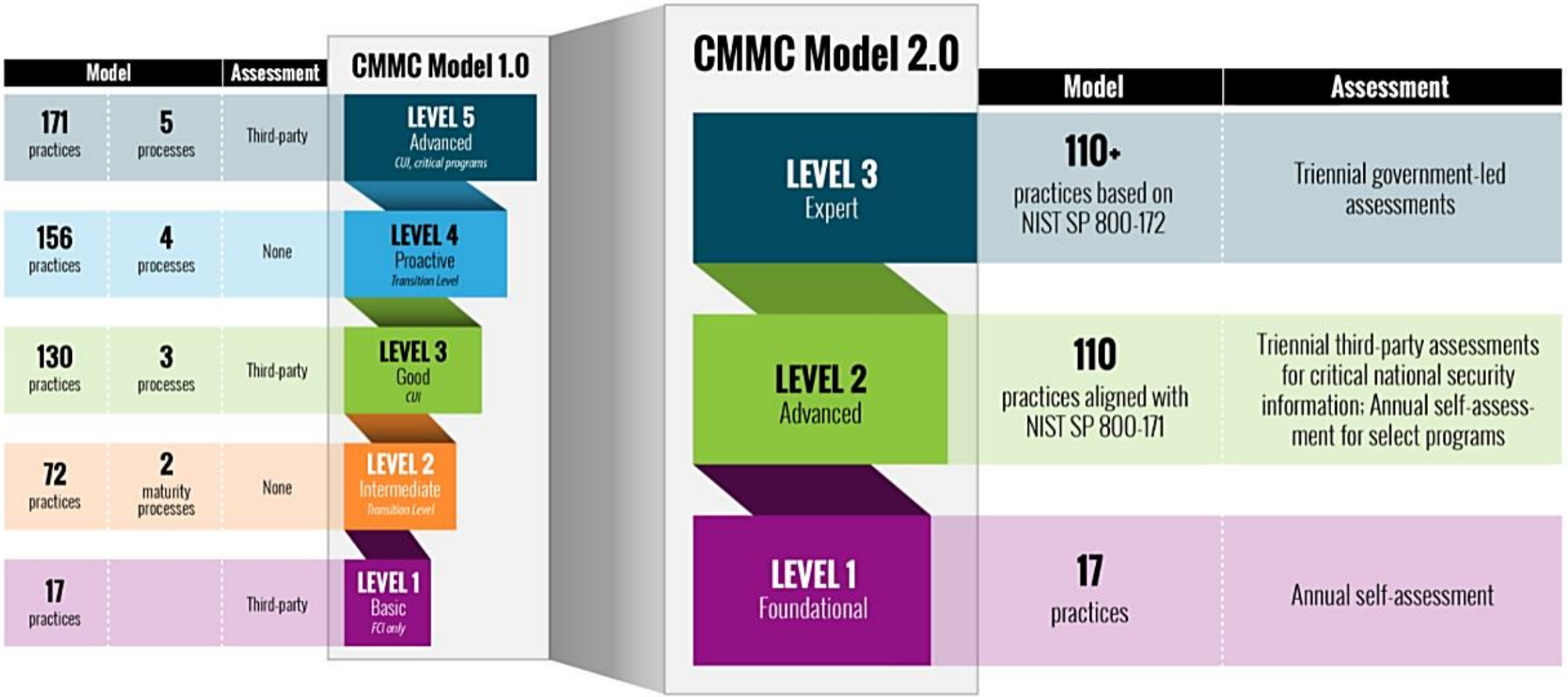
- The standards today are preparing us for the CMMC.
  - Federal Acquisition Regulation (FAR) 52.204-21 "Basic Safeguarding of Covered Contract Information Systems"
    - Mandatory flowdown in contracts, 15 basic security controls
  - Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012 "Safeguarding Covered Defense Information and Cyber Incident Reporting"
    - Self attestation of System Security Plan outlining the implementation of NIST SP 800-171
  - 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 via Self reporting/Third Party/Government in accordance with the NIST SP 800-171

What's Next?

- Updates to the FAR are anticipated to take place to include more stringent cybersecurity requirements, similar to those in the DFARS.

Cybersecurity Maturity Model Certification (CMMC)

Cybersecurity Maturity Model Certification (CMMC)



CMMC 2.0

With the implementation of CMMC 2.0, the Department is introducing several key changes that build on and refine the original program requirements. These are:

Streamlined Model

- ***Focused on the most critical requirements:*** Streamlines the model from 5 to 3 compliance levels
- ***Aligned with widely accepted standards:*** Uses National Institute of Standards and Technology (NIST) cybersecurity standards

Reliable Assessments

- ***Reduced assessment costs:*** Allows all companies at Level 1 (Foundational), and a subset of companies at Level 2 (Advanced) to demonstrate compliance through self-assessments
- ***Higher accountability:*** Increases oversight of professional and ethical standards of third-party assessors

Flexible Implementation

- ***Spirit of collaboration:*** Allows companies, under certain limited circumstances, to make Plans of Action & Milestones (POA&Ms) to achieve certification
- ***Added flexibility and speed:*** Allows waivers to CMMC requirements under certain limited circumstances

Requirements

I'm a company that handles CUI…how do I prepare for CMMC Level 2?

Start Here

- System Security Plan (SSP)
- NIST SP 800-171A
- FIPS-140 Encryption
- Engage with DIB/Peers
- Multifactor Authentication
- Documentation and Policies

CMMC Small Business Impact

- Small Business Impact:
  - Section 848 requires the DoD to examine the potential impacts of CMMC on small businesses and deliver, within 120 days, a report, specifically detailing: "(1) the estimated costs of complying with each level of the [CMMC] framework; (2) any decrease in the number of small business concerns that are part of the defense industrial base resulting from the implementation and use of the framework; and (3) an explanation of how the DoD will mitigate the negative effects to small business concerns that are part of the defense industrial base resulting from the implementation

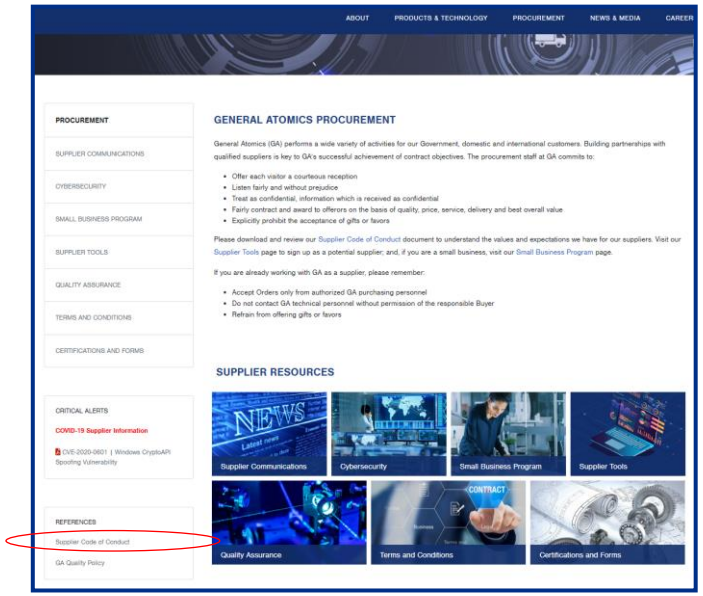
Cybersecurity

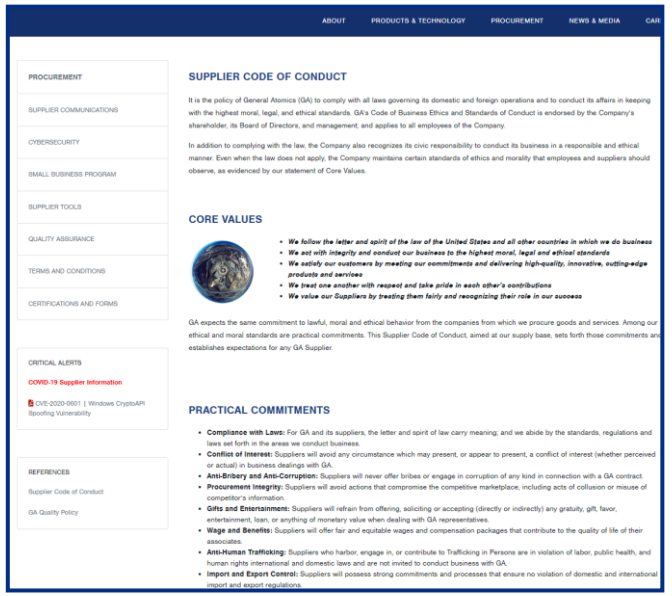
Supplier Resources

GENERAL ATOMICS

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.





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.

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 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 chain accountability.

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.

Supplier Resources

The Future

Preparing for the Cybersecurity Maturity Model Certification (CMMC)

Is your company ready for the CMMC?

The Department of Defense (DoD) Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD A&S) 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 January 31, 2020, CMMC was introduced as a critical step toward meeting this goal.

The CMMC model "combines various Cybersecurity standards and best practices and maps these controls and processes across several maturity levels that range from basic cyber hygiene to advanced." Each CMMC level introduces additional security controls and processes that, when implemented, enhance the Cybersecurity posture of the organization and protect against progressively sophisticated cyber threats.

GA Suppliers that handle FCI, CDI or CUI will be required to implement the CMMC at the level commensurate with the type of information being handled.

CMMC builds upon existing requirements in the Federal Acquisition Regulation (FAR) 52.204-21 "Basic Safeguarding of Covered Contractor Information Systems" and the Defense Federal Acquisition Regulations Supplement (DFARS) 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting".

In November of 2021, the Department of Defense announced an updated structure to CMMC, calling it CMMC 2.0. Review the latest news at the Acquisition and Sustainment Office of the Under Secretary of Defense website.

Questions