GENERAL DYNAMICS
Mission Systems

DoD Cybersecurity
Pittsfield Small Business Event
Joanne Chabot

June 27, 2022

Topics

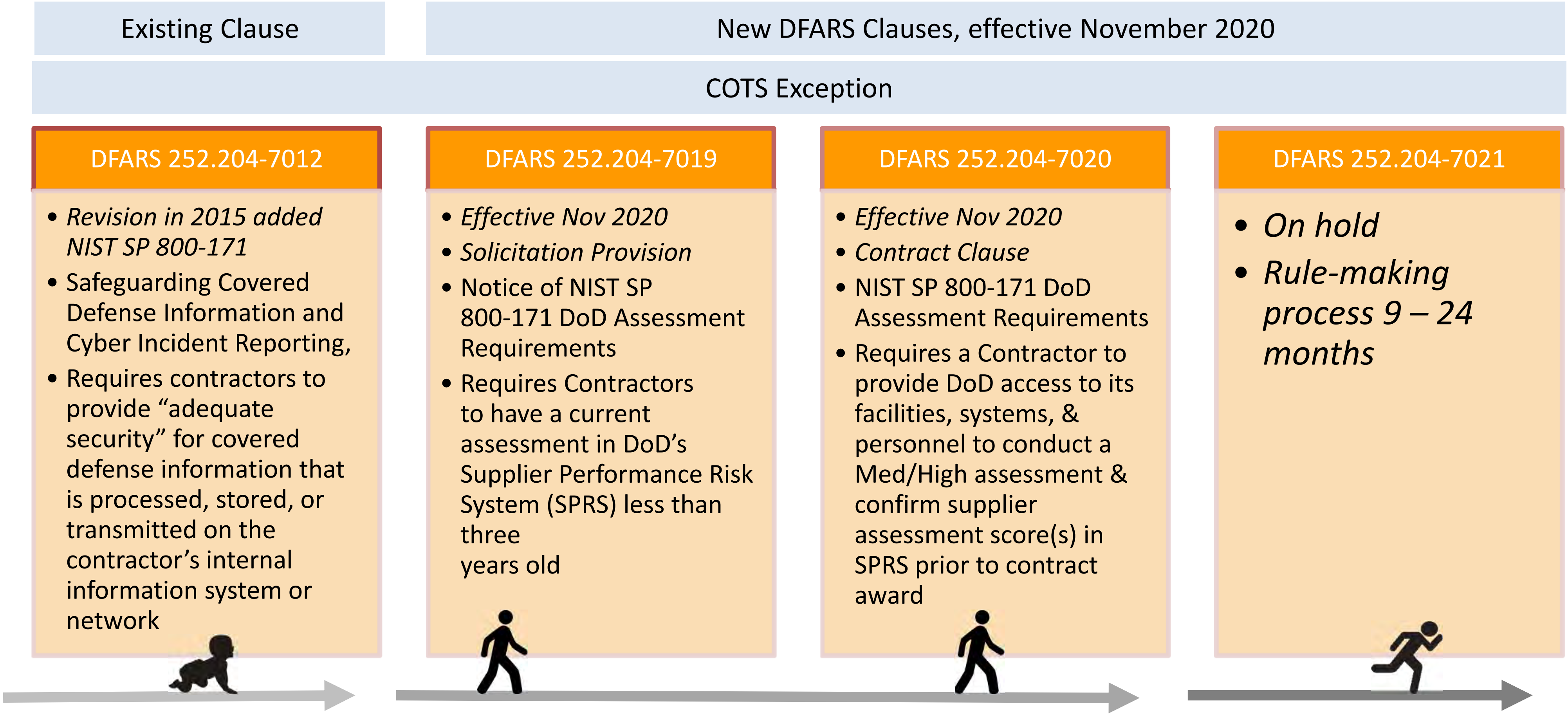
- Background
- FAR 52.204-21 and DFARS 252.204-7012
- Covered Defense Information and Controlled Unclassified Information
- Cybersecurity Maturity Model Certification (CMMC) 2.0
- Compliance
- Resources
- Take-Aways
- Questions
- Back-up – Additional Information

Background

- **Cybersecurity is a top priority for the Department of Defense**
- Theft of intellectual property and sensitive information due to malicious cyber activity threatens economic security and national security
- Defense contractors must view cybersecurity as part of doing business in order to protect themselves and to protect national security
- DoD developed an assessment methodology and framework to assess contractor implementation of cybersecurity requirements –
  - National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 DoD Assessment Methodology, and
  - Cybersecurity Maturity Model Certification (CMMC) Framework

CISA recommends all organizations – regardless of size – adopt a heightened posture when it comes to cybersecurity and protecting their most critical assets.
Shields Up | CISA

DFARS Clauses: CMMC “Crawl-Walk-Run”



Existing Clause

New DFARS Clauses, effective November 2020

COTS Exception

DFARS 252.204-7012

- *Revision in 2015 added NIST SP 800-171*
- Safeguarding Covered Defense Information and Cyber Incident Reporting,
- Requires contractors to provide “adequate security” for covered defense information that is processed, stored, or transmitted on the contractor’s internal information system or network

DFARS 252.204-7019

- *Effective Nov 2020*
- *Solicitation Provision*
- Notice of NIST SP 800-171 DoD Assessment Requirements
- Requires Contractors to have a current assessment in DoD’s Supplier Performance Risk System (SPRS) less than three years old

DFARS 252.204-7020

- *Effective Nov 2020*
- *Contract Clause*
- NIST SP 800-171 DoD Assessment Requirements
- Requires a Contractor to provide DoD access to its facilities, systems, & personnel to conduct a Med/High assessment & confirm supplier assessment score(s) in SPRS prior to contract award

DFARS 252.204-7021

- *On hold*
- *Rule-making process 9 – 24 months*

DFARS 252.204-7012 - Summary

Safeguarding Covered Defense Information and Cyber Incident Reporting

SECURITY

- Provide adequate security to safeguard Covered Defense Information (CDI) that resides on or is transiting though a contractor's internal information system or network
- Comply with the National Institute of Standards and Technology (NIST) special Publications (SP) 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations
  (110 requirements)
- Demonstrate implementation or planned implementations of the security requirements through a "System Security Plan" (SSP) and associated "Plan of Action and Milestones" (POAM)
- Contractors may submit requests to vary from NIST SP 800-171 (N/A or alternatives)

REPORT

- Report cyber incidents within 72 hours
- Submit malicious software discovered and isolated in connection with a reported cyber incident to the DoD Cyber Crime Center
- If requested, submit media and additional information to support damage assessment

CLOUD

- If using a Cloud Service Provider (CSP) to store, process or transmit CDI in performance of the contract, the CSP must meet the Government's FedRAMP Moderate baseline requirements

FLOW DOWN

- Flow down the clause in subcontracts for operational critical support, or for which subcontract performance will involve CDI

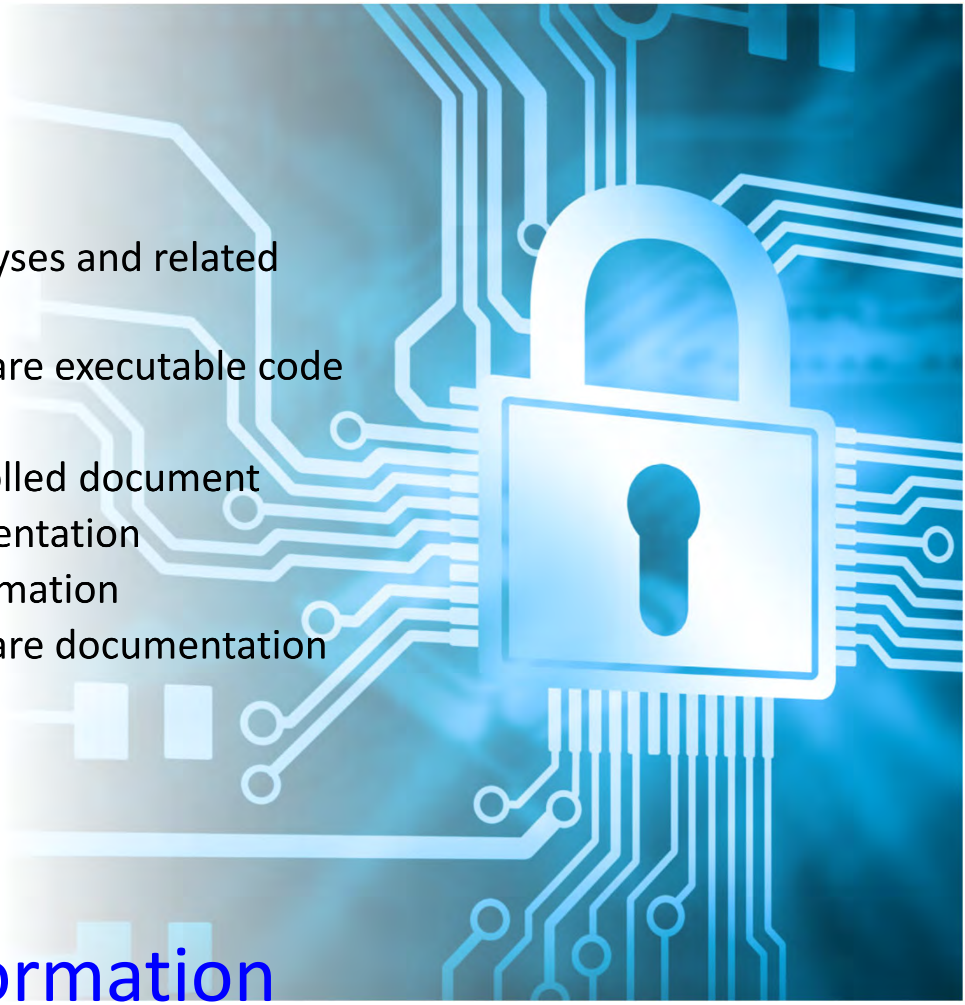
DFARS 252.204-7012

- • “Covered defense information” means unclassified controlled technical information **or** other information, as described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, and is—
- (1) Marked or otherwise identified 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

Two important “or” phases!

GENERAL DYNAMICS
Mission Systems

Examples of CUI



- Research and engineering data
- Engineering drawings
- Associated engineering lists
- Specifications
- Standards
- Process sheets
- Manuals
- Technical reports
- Technical orders
- Catalog-item identifications

- Data sets
- Studies and analyses and related information
- Computer software executable code
- Source Code
- An export-controlled document
- Software documentation
- Proprietary information
- Computer software documentation

Resources (includes marking guidance):

DoD CUI Training

DCSA Controlled Unclassified Information

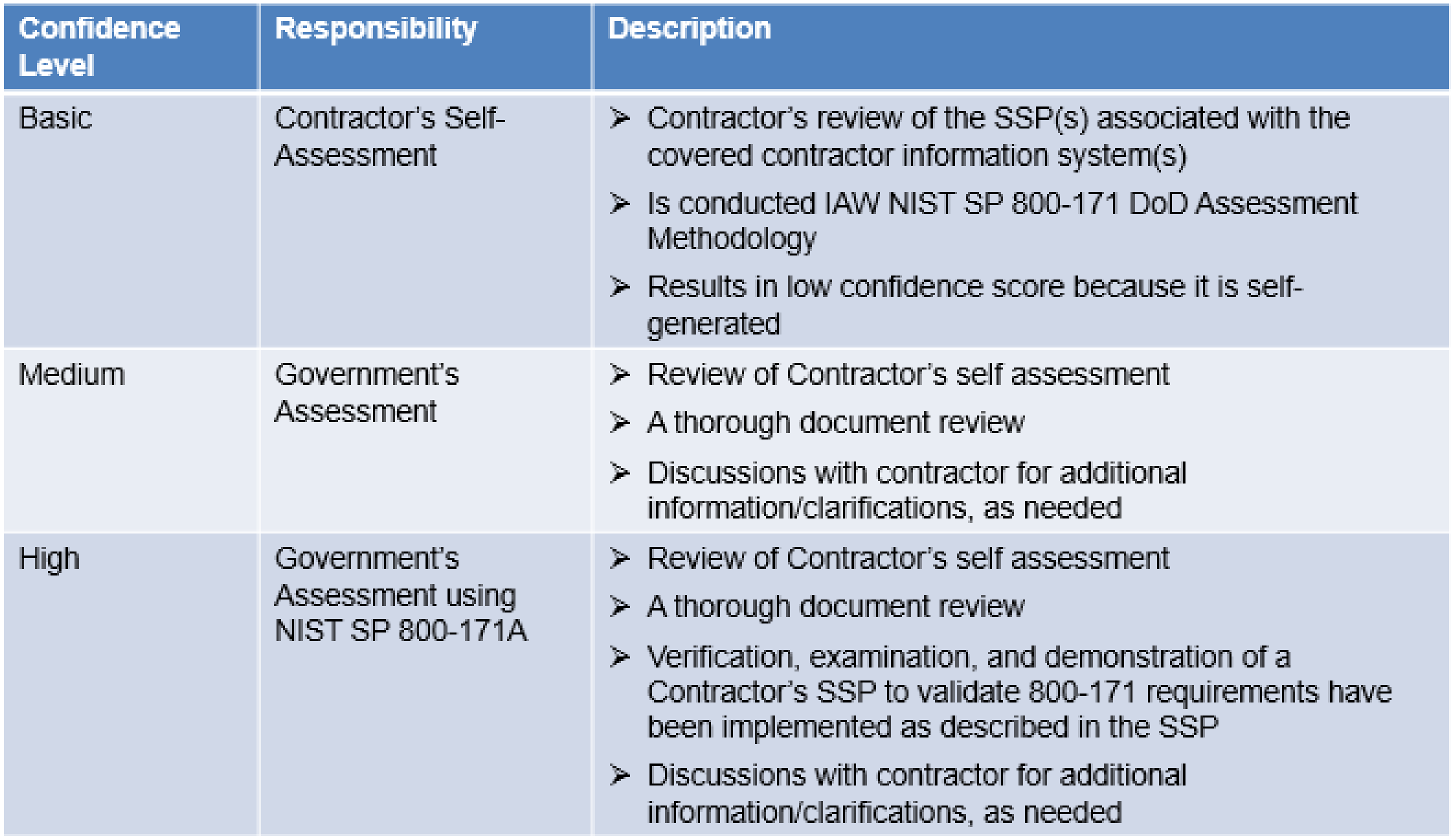
What is NOT CUI?

- Public Information
  - Information that is lawfully publicly available without restrictions
  - For example, a document marked “Public Release – No Dissemination Limitation”
- Commercially Available Off-The-Shelf (COTS) Item Information
  - Information must be solely related to COTS
- Internal Contractor Information that is incidental to contract performance
  - For example, human resources or financial information
- Classified Information

DFARS 252.204-7020 NIST SP 800-171 DoD Assessment Requirements (Cont.)

- Subcontracts
  - Required flow down, including the acquisition of commercial items
  - Exceptions: Solely COTS or acquisitions at/below the micro-purchase threshold (currently $10,000)
  - Contractor is **prohibited** from awarding a subcontract or other contractual instrument subject to NIST SP 800-171 security requirements, unless the subcontractor has completed, within the last 3 years, at least a Basic NIST SP 800-171 DoD Assessment
  - If a subcontractor does not have summary level scores of a current Assessment posted in SPRS, the subcontractor may conduct and submit a Basic Assessment in accordance with NIST SP 800-171 DoD Assessment Methodology, to webptsmh@navy.mil for posting to SPRS or submit its Basic Assessment score directly in SPRS

DFARS 252.204-7020 NIST SP 800-171 DoD Assessment Requirements (Cont.)



Confidence Level	Responsibility	Description
Basic	Contractor's Self-Assessment	➢ Contractor's review of the SSP(s) associated with the covered contractor information system(s) ➢ Is conducted IAW NIST SP 800-171 DoD Assessment Methodology ➢ Results in low confidence score because it is self-generated
Medium	Government's Assessment	➢ Review of Contractor's self assessment ➢ A thorough document review ➢ Discussions with contractor for additional information/clarifications, as needed
High	Government's Assessment using NIST SP 800-171A	➢ Review of Contractor's self assessment ➢ A thorough document review ➢ Verification, examination, and demonstration of a Contractor's SSP to validate 800-171 requirements have been implemented as described in the SSP ➢ Discussions with contractor for additional information/clarifications, as needed

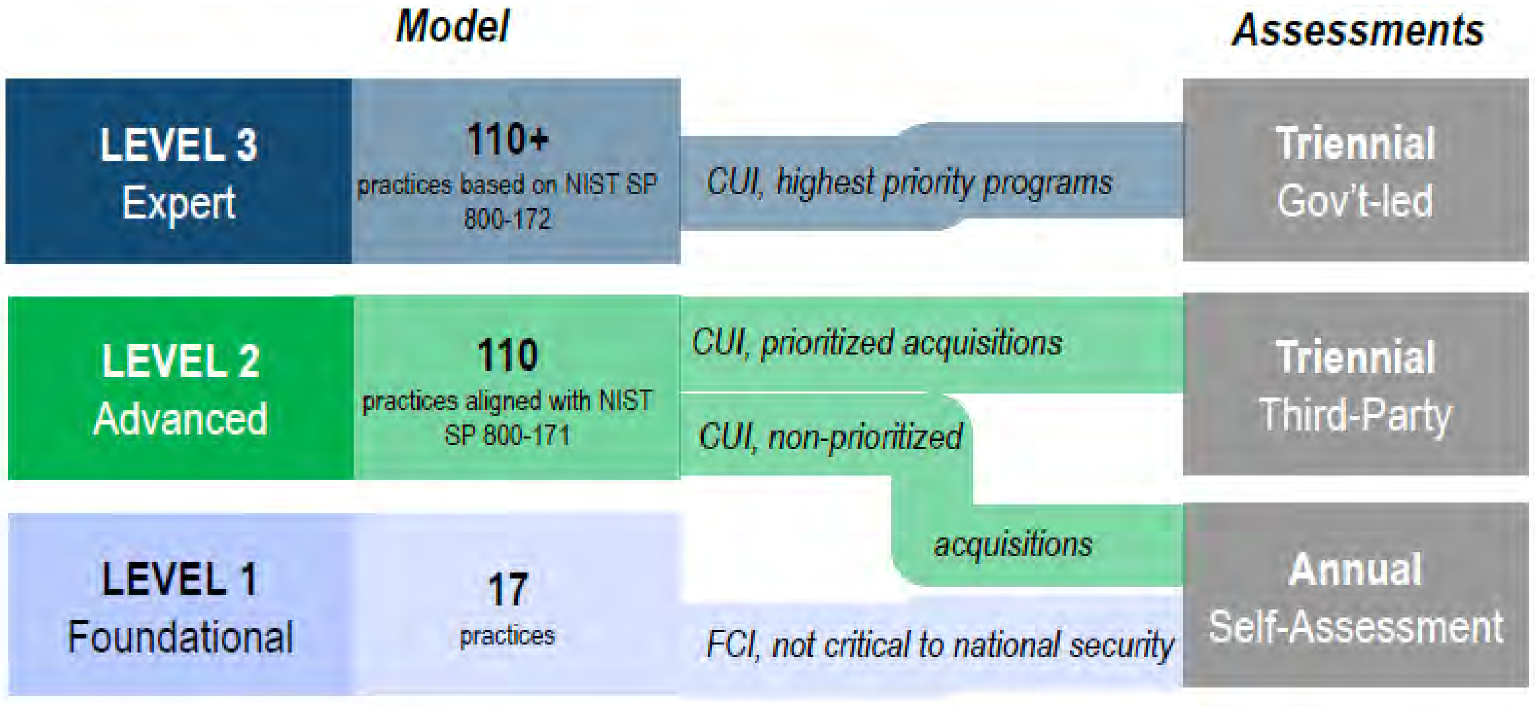
Cybersecurity Maturity Model Certification (CMMC) Program

- Background
  - In 2021, DoD put the CMMC program on hold while it reviewed over 850 public comments in response to the CMMC 1.0 interim DFARS rule
  - CMMC 1.0 had five maturity levels, ranging from Level 1 (Basic) to Level 5 (Advanced)
    - ❑ CMMC level 3 included CUI security requirements from NIST SP 800-171 (110 requirements) specified in DFARS 252.204-7012, plus 20 additional practices
    - ❑ All five levels required third-party certification
    - ❑ No POAMs were permitted to achieve certification
- On November 4, 2021, DoD announced CMMC 2.0
  - A comprehensive framework to protect the defense industrial base from increasingly frequent and complex cyberattacks. With its streamlined requirements, CMMC 2.0:
    - ❑ Cuts red tape for small and medium sized businesses
    - ❑ Sets priorities for protecting DoD information
    - ❑ Reinforces cooperation between the DoD and industry in addressing evolving cyber threats

CMMC 2.0 - Streamlined

- Streamlined Model – Reduced from 5 to 3 compliance levels, eliminates CMMC 1.0 Levels 2 and 4
  - Aligned with NIST cybersecurity standards – widely accepted standards
- Establishes three progressively sophisticated levels, depending on the type of information:
  - Level 1 (Foundational) – for companies with Federal Contract Information (FCI) only; information requires protection but is not critical to national security
  - Level 2 (Advanced) – for companies with CUI
  - Level 3 (Expert) – for the highest priority programs with CUI
- Requirements will mirror NIST SP 800-171 and NIST SP 800-172, Enhanced Security Requirements for Protecting CUI: A Supplement to NIST SP 800-171
  - Eliminates all CMMC unique practices and maturity processes
  - Aligns Level 2 with NIST SP 800-171 which is required for DFARS 252.204-7012
  - Level 3 will use a subset of NIST SP 800-172 requirements

CMMC 2.0 – Tailors model & assessment requirements to type of information being handled



Model

Assessments

LEVEL 3
Expert

110+
practices based on NIST SP 800-172

CUI, highest priority programs

Triennial
Gov't-led

LEVEL 2
Advanced

110
practices aligned with NIST SP 800-171

CUI, prioritized acquisitions

CUI, non-prioritized acquisitions

Triennial
Third-Party

LEVEL 1
Foundational

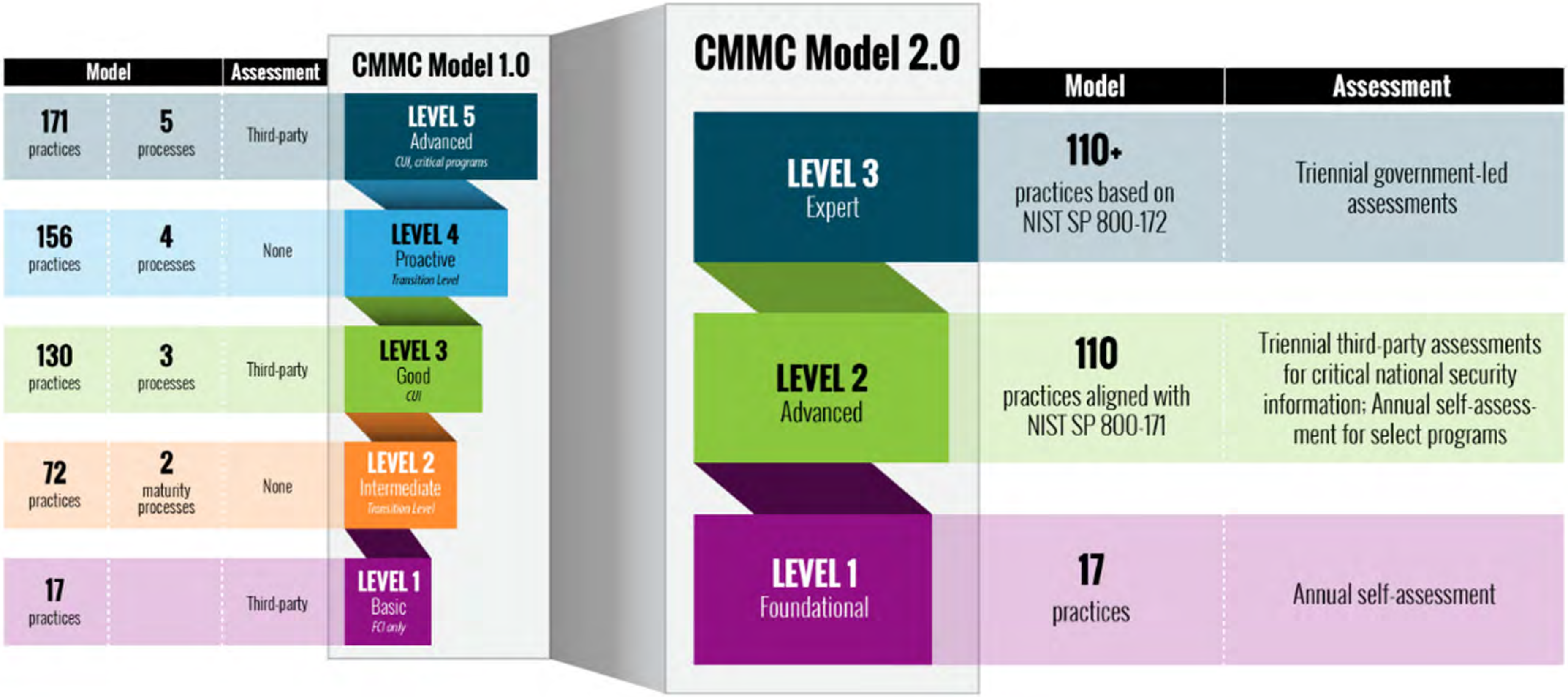
17
practices

FCI, not critical to national security

Annual
Self-Assessment

Program details are subject to change during rulemaking and internal resourcing as part of implementation.

KEY FEATURES OF CMMC 2.0



CMMC Model 1.0

Model		Assessment	CMMC Model 1.0
171 practices	5 processes	Third-party	LEVEL 5 Advanced *CUI, critical programs*
156 practices	4 processes	None	LEVEL 4 Proactive *Transition Level*
130 practices	3 processes	Third-party	LEVEL 3 Good *CUI*
72 practices	2 maturity processes	None	LEVEL 2 Intermediate *Transition Level*
17 practices		Third-party	LEVEL 1 Basic *FCI only*

CMMC Model 2.0

CMMC Model 2.0	Model	Assessment
LEVEL 3 Expert	110+ practices based on NIST SP 800-172	Triennial government-led assessments
LEVEL 2 Advanced	110 practices aligned with NIST SP 800-171	Triennial third-party assessments for critical national security information; Annual self-assessment for select programs
LEVEL 1 Foundational	17 practices	Annual self-assessment

CMMC 2.0 – Allowance of POAMs and Waivers

- Allows limited use of POAMs
  - Time-bound – potentially 180 days
  - Limited use – no POAMs for highest-weighted requirements; will establish a minimum score required to support certification with POAMs
- Waivers permitted on very limited basis with strategies to mitigate CUI risk
  - Only allowed in select mission critical instances
    - ❑ Government program office will submit waiver request with justification and risk mitigation
  - Strictly time bound
    - ❑ Timing determined on case-by-case basis
  - Requires senior DoD approval to minimize potential misuse of the waiver process

Limited use of POAMs and waivers could allow DoD and Contractors flexibility to meet evolving threats and make risk-based decisions.

CMMC 2.0 – Rulemaking; Codifying CMMC 2.0

- Changes will be released through an interim rule
  - Anticipate revisions to DFARS 252.204-7021 Cybersecurity Maturity Model Certification Requirements
  - Timeline to complete all rule-making requirements will be 9 – 24 months
  - A 60-day public comment period and concurrent congressional review will be included prior to the rule becoming effective
- DoD suspended the CMMC Piloting effort and mandatory CMMC certification
- DIB contractors are encouraged to enhance their cybersecurity posture during this period

Supply Chain Management (SCM) Compliance Approach

- SCM updated supplier flow downs, as required
- GDMS external supplier site is updated to include the new requirements
- SCM issues a supplier representation and certification regarding a supplier's current Assessment(s) posted in SPRS
  - A supplier representation and certification is necessary, because GDMS does not have access to a supplier's information in SPRS
  - The representation and certification includes a link to GDMS external supplier site
- SCM issued a communication to suppliers with the new representation and certification

SCM Compliance Approach (Cont.)

- **For new DoD awards with the flow-downs**, SCM will confirm receipt of the completed representation and certification that the supplier has a current (within the last 3 years) Assessment posted on SPRS, prior to awarding a DoD purchase order or subcontract
  - Exceptions for solely COTS* procurements or procurements at or below the micro-purchase threshold ($10,000)
  - SCM will review supplier’s assessment score and based on score may ask if supplier will share its System Security Plan and Plan of Action and Milestones

Commercially available off-the-shelf (COTS) item*— A commercial item 1) **sold in substantial quantities in the commercial marketplace; and 2) offered to the Government, under a contract or subcontract at any tier, **without modification**, in the same form in which it is sold in the commercial marketplace.

SCM Compliance Approach (Cont.)

- A supplier's status is included on GDMS Supplier 360
- A supplier needs a CAGE code to post an assessment on SPRS
  - Some suppliers do not have CAGE codes and are not registered in the U.S. Government's (USG) System for Award Management, because they do not perform work directly for the USG
  - Information regarding registration in SAM and CAGE codes is available at: https://sam.gov/SAM/pages/public/generalInfo/aboutSAM.jsf
  - Establishing a CAGE code may take several weeks
- SCM has issued articles in the Innovative Sourcing newsletter to suppliers regarding the new DFARS cybersecurity requirements

- SCM has issued articles in the Innovative Sourcing newsletter to suppliers regarding the new DFARS cybersecurity requirements

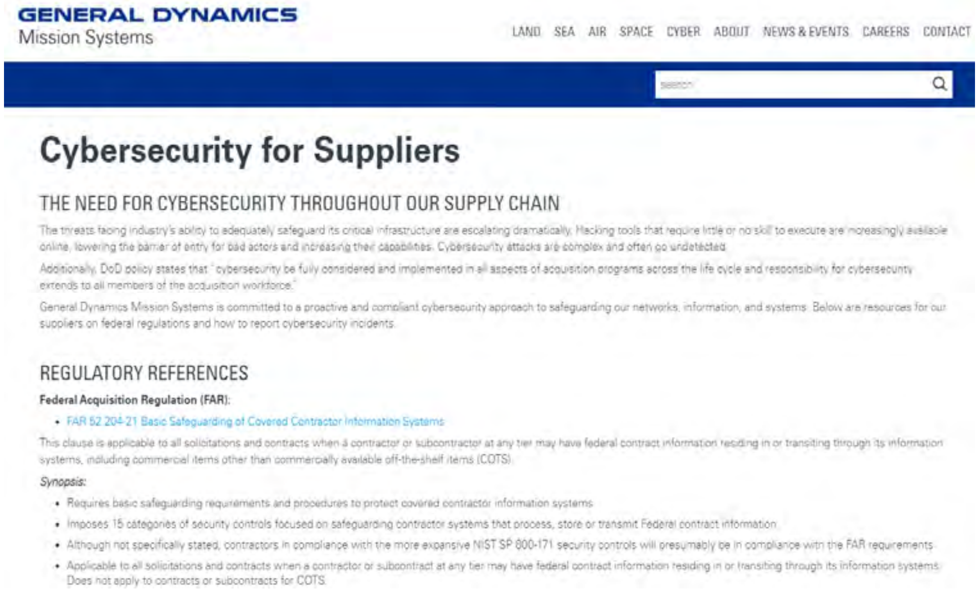
- SCM participates in various small business conferences and industry meetings with will spread awareness
- ***Important Reminder*** - Suppliers receiving CUI must be compliant with DFARS 252.204-7012 regardless of dollar value of award
  - COTS exemption only

Supplier Actions – If not yet completed

- Complete representation and certification to GDMS for both DFARS 252.204-7012 and 252.204-7020
- Ensure that the Supplier has a System Security Plan (SSP) in place to describe how the security controls are implemented, in addition to associated Plan of Action and Milestones (POAMs) to describe how and when unimplemented security requirements will be met (DFARS 252.204-7012)
  - NIST: CUI Plan of Action Template
  - NIST: CUI SSP Template
- Complete at least a Basic Assessment in accordance with NIST SP 800-171 DoD Assessment Methodology (DFARS 252.204-7020)
  - NIST SP 800-171 DoD Assessment Methodology
  - Enter assessment into SPRS
    - ❑ Obtain a CAGE code if you do not already have one

Cybersecurity for Suppliers

- Reference information posted on GDMS public domain site, http://gdmissionsystems.com
- Regulatory References
- Reporting a Cybersecurity Incident
- Links to other helpful resources


GENERAL DYNAMICS
Mission Systems
LAND SEA AIR SPACE CYBER ABOUT NEWS & EVENTS CAREERS CONTACT
search

Cybersecurity for Suppliers

THE NEED FOR CYBERSECURITY THROUGHOUT OUR SUPPLY CHAIN

The threats facing industry's ability to adequately safeguard its critical infrastructure are escalating dramatically. Hacking tools that require little or no skill to execute are increasingly available online, lowering the barrier of entry for bad actors and increasing their capabilities. Cybersecurity attacks are complex and often go undetected.

Additionally, DoD policy states that "cybersecurity be fully considered and implemented in all aspects of acquisition programs across the life cycle and responsibility for cybersecurity extends to all members of the acquisition workforce."

General Dynamics Mission Systems is committed to a proactive and compliant cybersecurity approach to safeguarding our networks, information, and systems. Below are resources for our suppliers on federal regulations and how to report cybersecurity incidents.

REGULATORY REFERENCES

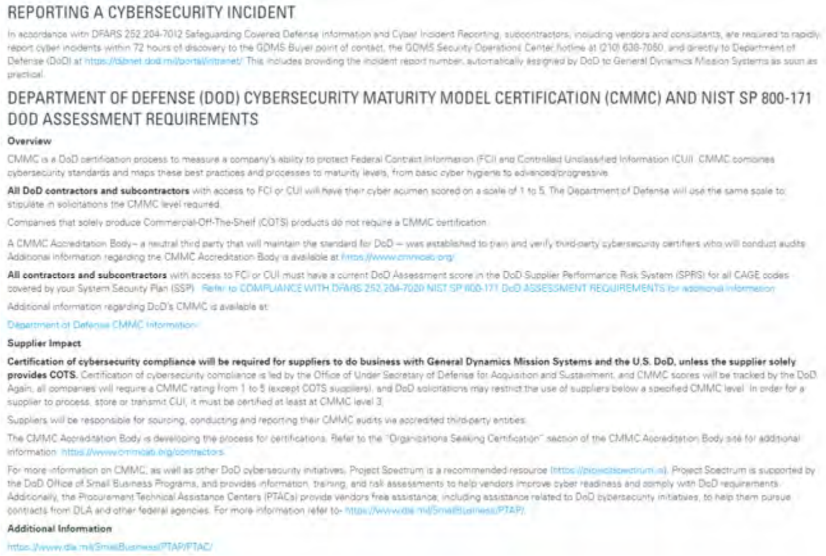
Federal Acquisition Regulation (FAR):

- FAR 52.204-21 Basic Safeguarding of Covered Contractor Information Systems

This clause is applicable to all solicitations and contracts when a contractor or subcontractor at any tier may have federal contract information residing in or transiting through its information systems, including commercial items other than commercially available off-the-shelf items (COTS).

Synopsis:

- Requires basic safeguarding requirements and procedures to protect covered contractor information systems
- Imposes 15 categories of security controls focused on safeguarding contractor systems that process, store or transmit Federal contract information
- Although not specifically stated, contractors in compliance with the more expansive NIST SP 800-171 security controls will presumably be in compliance with the FAR requirements
- Applicable to all solicitations and contracts when a contractor or subcontract at any tier may have federal contract information residing in or transiting through its information systems. Does not apply to contracts or subcontracts for COTS.



REPORTING A CYBERSECURITY INCIDENT

In accordance with DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting, subcontractors, including vendors and consultants, are required to rapidly report cyber incidents within 72 hours of discovery to the GDMS Buyer point of contact, the GDMS Security Operations Center hotline at (210) 638-7050, and directly to Department of Defense (DoD) at https://dibnet.dod.mil/portal/intranet/. This includes providing the incident report number, automatically assigned by DoD to General Dynamics Mission Systems as soon as practical.

DEPARTMENT OF DEFENSE (DOD) CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) AND NIST SP 800-171 DOD ASSESSMENT REQUIREMENTS

Overview

CMMC is a DoD certification process to measure a company's ability to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). CMMC combines cybersecurity standards and maps these best practices and processes to maturity levels, from basic cyber hygiene to advanced/progressive.

All DoD contractors and subcontractors with access to FCI or CUI will have their cyber acumen scored on a scale of 1 to 5. The Department of Defense will use the same scale to stipulate in solicitations the CMMC level required.

Companies that solely produce Commercial-Off-The-Shelf (COTS) products do not require a CMMC certification.

A CMMC Accreditation Body – a neutral third party that will maintain the standard for DoD – was established to train and verify third-party cybersecurity certifiers who will conduct audits. Additional information regarding the CMMC Accreditation Body is available at https://www.cmmcab.org/

All contractors and subcontractors with access to FCI or CUI must have a current DoD Assessment score in the DoD Supplier Performance Risk System (SPRS) for all CAGE codes covered by your System Security Plan (SSP). Refer to COMPLIANCE WITH DFARS 252.204-7020 NIST SP 800-171 DoD ASSESSMENT REQUIREMENTS for additional information

Additional information regarding DoD's CMMC is available at:

Department of Defense CMMC Information

Supplier Impact

Certification of cybersecurity compliance will be required for suppliers to do business with General Dynamics Mission Systems and the U.S. DoD, unless the supplier solely provides COTS. Certification of cybersecurity compliance is led by the Office of Under Secretary of Defense for Acquisition and Sustainment, and CMMC scores will be tracked by the DoD. Again, all companies will require a CMMC rating from 1 to 5 (except COTS suppliers), and DoD solicitations may restrict the use of suppliers below a specified CMMC level. In order for a supplier to process, store or transmit CUI, it must be certified at least at CMMC level 3.

Suppliers will be responsible for sourcing, conducting and reporting their CMMC audits via accredited third-party entities.

The CMMC Accreditation Body is developing the process for certifications. Refer to the "Organizations Seeking Certification" section of the CMMC Accreditation Body site for additional information: https://www.cmmcab.org/contractors.

For more information on CMMC, as well as other DoD cybersecurity initiatives, Project Spectrum is a recommended resource (https://projectspectrum.io). Project Spectrum is supported by the DoD Office of Small Business Programs, and provides information, training, and risk assessments to help vendors improve cyber readiness and comply with DoD requirements. Additionally, the Procurement Technical Assistance Centers (PTACs) provide vendors free assistance, including assistance related to DoD cybersecurity initiatives, to help them pursue contracts from DLA and other federal agencies. For more information refer to- https://www.dla.mil/SmallBusiness/PTAP/.

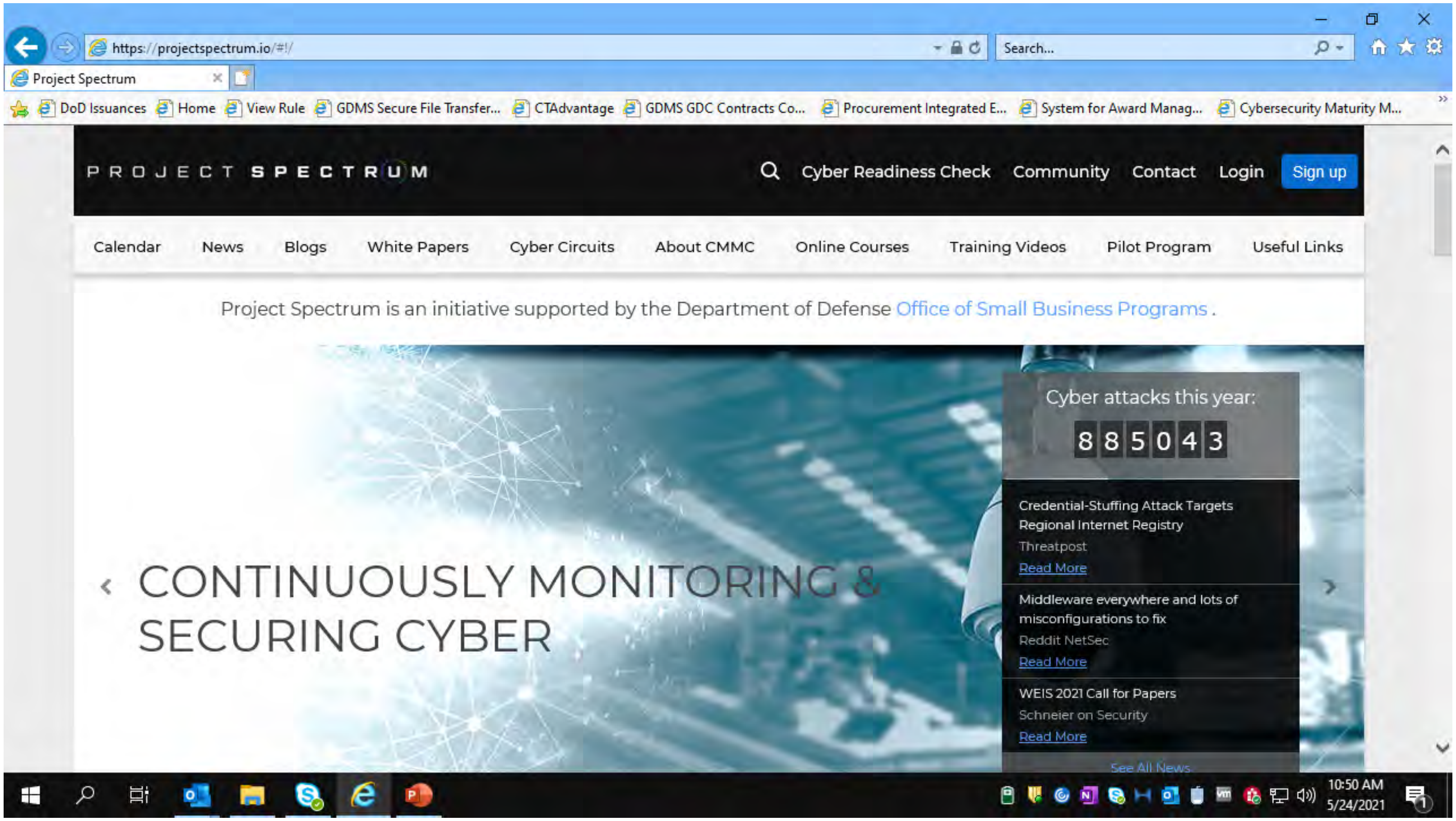
Additional Information

https://www.dla.mil/SmallBusiness/PTAP/PTAC/

Resources

- DoD CMMC
- DoD CUI
- DoD Procurement Toolbox
- Defense Counterintelligence and Security Agency CUI
- Project Spectrum - Supported by DoD Small Business Programs
- Federal Register Notice - Interim DFARS Rule
- CMMC Accreditation Body

Project Spectrum



Project Spectrum is an initiative supported by the Department of Defense Office of Small Business Programs .

CONTINUOUSLY MONITORING & SECURING CYBER

Cyber attacks this year:

885043

Credential-Stuffing Attack Targets Regional Internet Registry
Threatpost
Read More

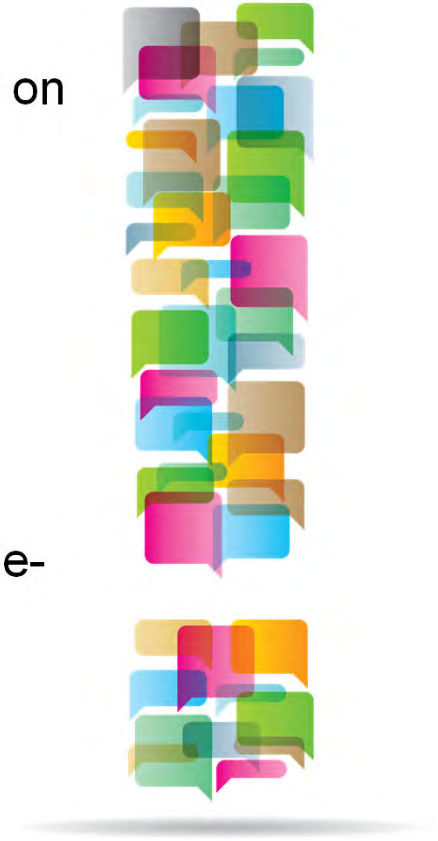
Middleware everywhere and lots of misconfigurations to fix
Reddit NetSec
Read More

WEIS 2021 Call for Papers
Schneier on Security
Read More

See All News

Take-Aways

- DoD Contractors, including Subcontracts/Suppliers, must have a current assessment for each covered contractor information posted on SPRS **to be eligible for award**
  - Enclaves used in contract performance require a current DoD assessment
  - ONLY exceptions are solely COTS and acquisitions at or below the micro-purchase threshold ($10K)
- For DoD Assessments, contractors can have a POAM to address gaps
- CMMC program is currently on hold while DoD goes through the rule-making process including congressional review
- Continue to monitor the rule-making process
- Cross-functional collaboration on cybersecurity requirements is essential



Questions

GENERAL DYNAMICS
Mission Systems