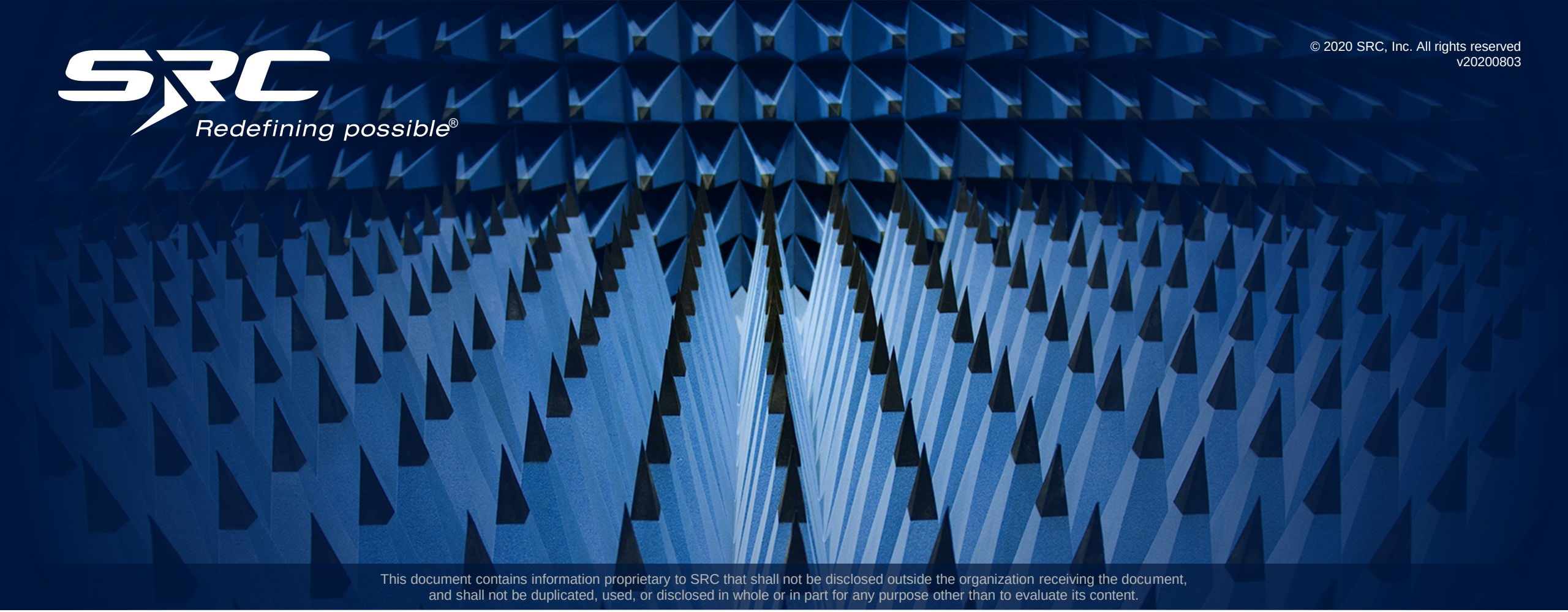


New Cyber Security Requirements for Contracts and Supply Chain

FY21

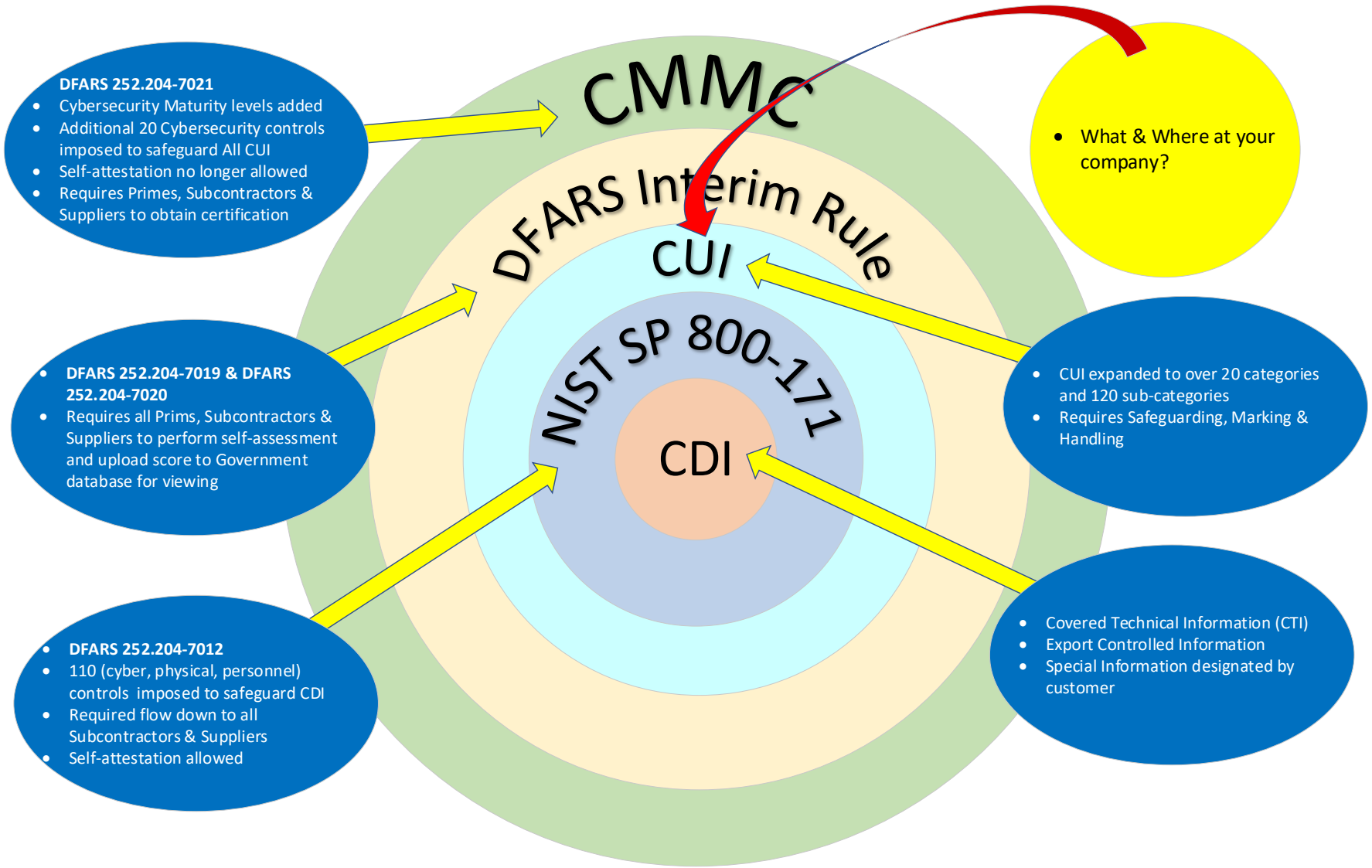
Objectives

- Our objectives today include:
  - Sharing information and raising awareness
  - Covering terminology and background
  - Fostering a common understanding
  - Discussing issues and answering questions
  - Planning forward
- These emerging requirements will impact the supply chain.

CMMC Background

- CMMC is the result of recent compromises of sensitive Government information.
- CMMC stands for Cyber Maturity Model Certification.
- CMMC Goal: Provide a single cybersecurity standard
  - CMMC combines multiple cybersecurity frameworks, including NIST Special Publication 800-171, into one unified set of benchmarks.
  - for All government agencies
  - to protect all CUI categories, not just those under CDI.
- DoD is the first agency to adopt CMMC.
  - No indication of when other agencies will adopt CMMC.
- You are either 100% compliant or considered non-compliant.

Overview


DFARS 252.204-7021
Cybersecurity Maturity levels added
Additional 20 Cybersecurity controls imposed to safeguard All CUI
Self-attestation no longer allowed
Requires Primes, Subcontractors & Suppliers to obtain certification
CMMC
DFARS Interim Rule
CUI
NIST SP 800-171
CDI
What & Where at your company?
DFARS 252.204-7019 & DFARS 252.204-7020
Requires all Prims, Subcontractors & Suppliers to perform self-assessment and upload score to Government database for viewing
CUI expanded to over 20 categories and 120 sub-categories
Requires Safeguarding, Marking & Handling
DFARS 252.204-7012
110 (cyber, physical, personnel) controls imposed to safeguard CDI
Required flow down to all Subcontractors & Suppliers
Self-attestation allowed
Covered Technical Information (CTI)
Export Controlled Information
Special Information designated by customer

CUI Definition

- Initiated under Executive Order 13556 in 2010.
- Controlled Unclassified Information (CUI) is information that requires safeguarding or dissemination controls.
- Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract

  -AND/OR-
- Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.
- Corporate intellectual property is not CUI, unless created for or included in requirements related to a government contract.

CDI Background

- CDI is a subset of CUI, which currently includes:
  - Defense - Controlled Technical Information (CTI)
    - » Controlled Technical Information (CTI) means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination pursuant to and consistent with law, regulations, and Government wide policies.
    - » Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code
  - Export Control – ITAR
    - » Unclassified information concerning certain items, commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives. To include dual use items; items identified in export administration regulations, international traffic in arms regulations and the munitions list; license applications; and sensitive nuclear technology information.
- Currently under DFARS 252.204-7012, companies are required to protect Covered Defense Information (CDI).

Existing DFARS

- DFARS 252.204-7012 in existing contracts
  - Add compliance requirement for protecting CDI under NIST SP 800-171.
  - Requires your self-attestation (when you sign the contract) that you are compliant.
    - » Non-compliant controls must be documented using Plans of Actions and Milestones (POA&Ms).
  - Requires someone at your company to be able to report cyber incidents using a Medium assurance certificate.

New DFARS prior to CMMC

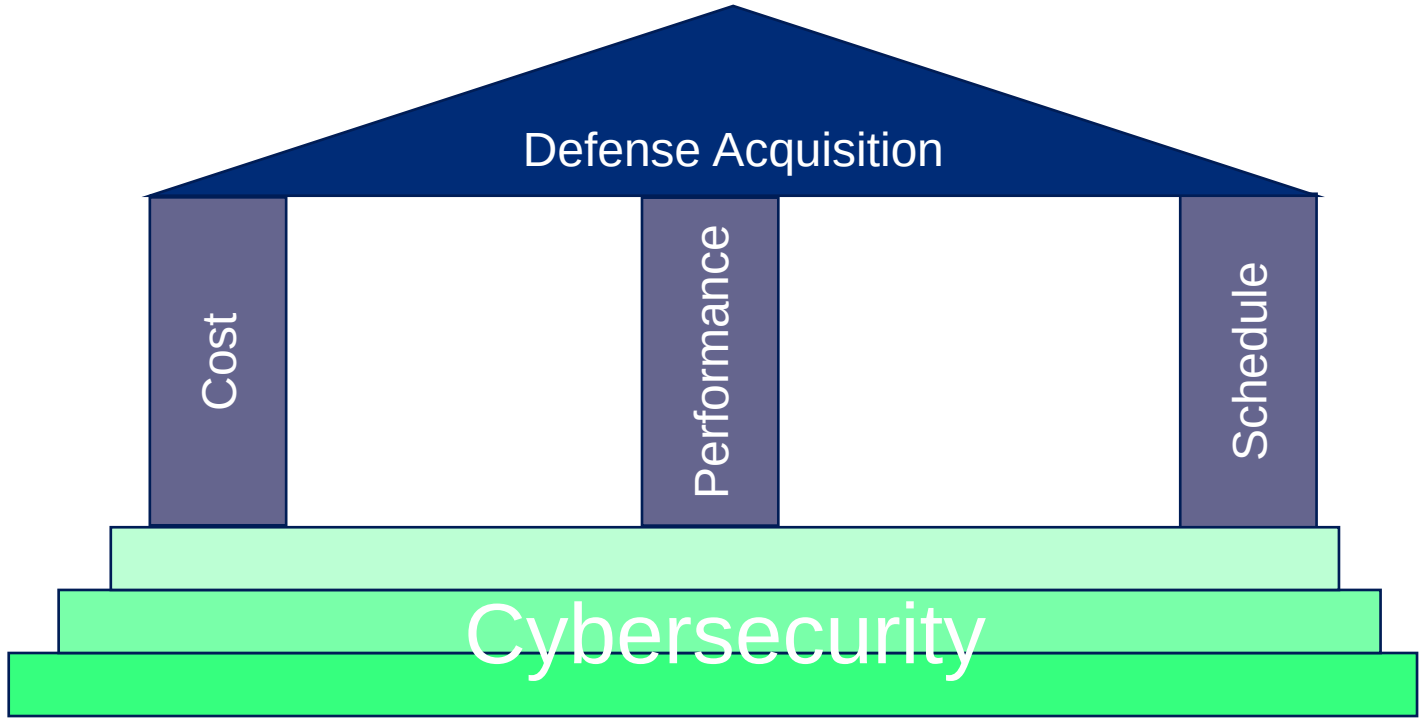
- Public comments for Interim Rule DFARS 2019-D041 ended November 30, 2020.
- DFARS 252.204-7019
  - Requires NIST SP 800-171A Self-Assessment
  - Score must be published in SPRS database
- DFARS 252.204-7020
  - Requires a contractor to provide the Government with access to its facilities, systems, and personnel when it is necessary for DoD to conduct or renew a higher-level Assessment.
  - Requires the contractor to ensure that applicable subcontractors also have the results of a current Assessment posted in SPRS prior to awarding a subcontract or other contractual instruments.
- DOD is currently in process of amending all existing contracts as quickly as possible with above clauses.

New DFARS for CMMC

- DFARS 252.204-7021 (Coming Soon)
  - Requires contractor to maintain the requisite CMMC level for the duration of the contract
  - Requires contractor to ensure subcontractors have the appropriate CMMC level prior to awarding a subcontract or other contractual instruments
  - Requires contractor to include the requirements of the clause in all subcontracts or other contractual instruments
- Currently affects NEW contract awards only
  - Currently CMMC is for NEW contracts only
    - » By FY26, all existing DOD contracts will have this requirement.
  - (15) pilot contracts to be identified in December 2020
  - *Please Note:* Classified Information/Data is out of scope and falls under RMF but there may be unclassified components of classified contracts.
- Affects everyone working on contract:
  - Prime → Tier 1 Suppliers → Tier 2 Suppliers
  - Excludes those used exclusively for the acquisition of COTS items (see COTS suppliers)

New Contracts with DFARS 252.204-7021

- Suppliers/Subcontractors must be certified at the required CMMC Level at the time of award.
- Non-Negotiable → This is a “Go/No Go” decision.



What is YOUR Target CMMC Level for FY21?

This depends on your contract(s)

- Are you providing COTS only?
  - certification not required
- Are you accessing, storing, or processing CUI (such as SRCXXXX or SCPXXXX parts)?
  - If yes, minimum Level 3
  - If no, but not considered COTS, minimum Level 1
- Less than 1% of all contracts will be Level 4 or 5

Certification

- Certification will be a requirement for all new DoD contracts.
- Contractors/suppliers must achieve their own certification.
  - Primes cannot certify you.
- Contractors/suppliers will have to get certified every three (3) years.
- Contractors/suppliers must be certified by contract award.
- COTS only suppliers do not require certification.

CMMC Business Impact

	Impact Description
Contract Award	• Applicable CMMC-level certification required for proposal to be considered
Certification Requirement	• Unlike NIST 800-171, cannot self-certify under CMMC • Any supplier/contractor with a direct contract with the Government must be Level 1 certified at a minimum • Primes must be certified at Level 3 minimum. • Contracts will dictate actual CMMC Level required.
Suppliers/Subcontractors	• Materials and Services must be procured from certified suppliers thus all Tier 1&2 suppliers/subcontractors must be certified to the same CMMC Level of the contract. • Primes cannot certify their own Tier 1&2 suppliers/subcontractors
Future Contracts	• Future work may be at risk depending on the CMMC level required by the contracting authority at recompete.

What this means to you as a supplier

- If your company does not apply sufficient resources (e.g., labor and material) you run the risk of not achieving certification.
- If your company isn’t certified, you can’t Bid/Win contracts with our company as a Tier 1 or Tier 2 supplier or subcontractor.
- If your suppliers and subcontractors are not certified, you may not be able to use them.
- If your company doesn’t protect CUI, you will lose contracts or lose the ability to bid on future contracts with our company.

IMMEDIATE Next Steps

- If you are delivering SRC designed parts or subcontract services, you are required to register with PIEE at https://piee.eb.mil/xhtml/unauth/home/login.xhtml
  - Perform a NIST SP 800-171A self-assessment
  - Upload your score to SPRS database
- Complete PIEE registration by December 1, 2020
- Provide to SRC the following:
  - Expected CMMC Level
  - PIEE Registration Number
  - Date of Registration

Next Steps - Prepare your organization for CMMC

- Identify programs with DFARS 252.204-7012
  - What CMMC Level does your company expect/want to be certified at?
- Identify your suppliers/subcontractors on each program
- Define scope of CUI within your company (if applicable)
  - Where is it?
  - Who has access to it?
- Identify resource needs to begin mitigating risks
- Implement CMMC controls (in addition to existing NIST SP 800-171 Controls)

CMMC Summary

- Be prepared in advance
  - Raise awareness within your company
  - Raise awareness with your suppliers/subcontractors
  - Begin planning now

Resources

- This slide deck will be available on the SRC internet site at https://srcinc.com/suppliers/
- For questions related to CMMC registration, certification and assessment, please visit the PIEE website at https://piee.eb.mil/xhtml/unauth/home/login.xhtml
- For more information on CMMC, please visit https://www.acq.osd.mil/cmmc/faq.html