Supply Chain Cybersecurity

Matthew A. Titcombe, CISSP, CCA, CCP
cmmc.services@peakinfosec.us
https://peakinfosec.com
(352) 897-3005

PUBLIC CONTRACTING INSTITUTE

A Bit About Me

- **Air Force & DoD Enterprise/Information Security Architect**
- **Air Force Program Manager at SAF/CIO and Air Force Academy**
- **Started Peak InfoSec in 2016**
- **CMMC Efforts:**
  - Provisional Assessor #17—now a CCA
  - CEO of an Authorized CMMC 3rd Party Assessor Organization (C3PAO)
  - CMMC Training Curriculum Developer
  - Including Peak InfoSec, involved in 4 DoD Audits related to NIST SP 800-171/CMMC in 2022
  - Serve as the Information System Security Officer for Coalfire Federal & led them through their CMMC audit

Agenda

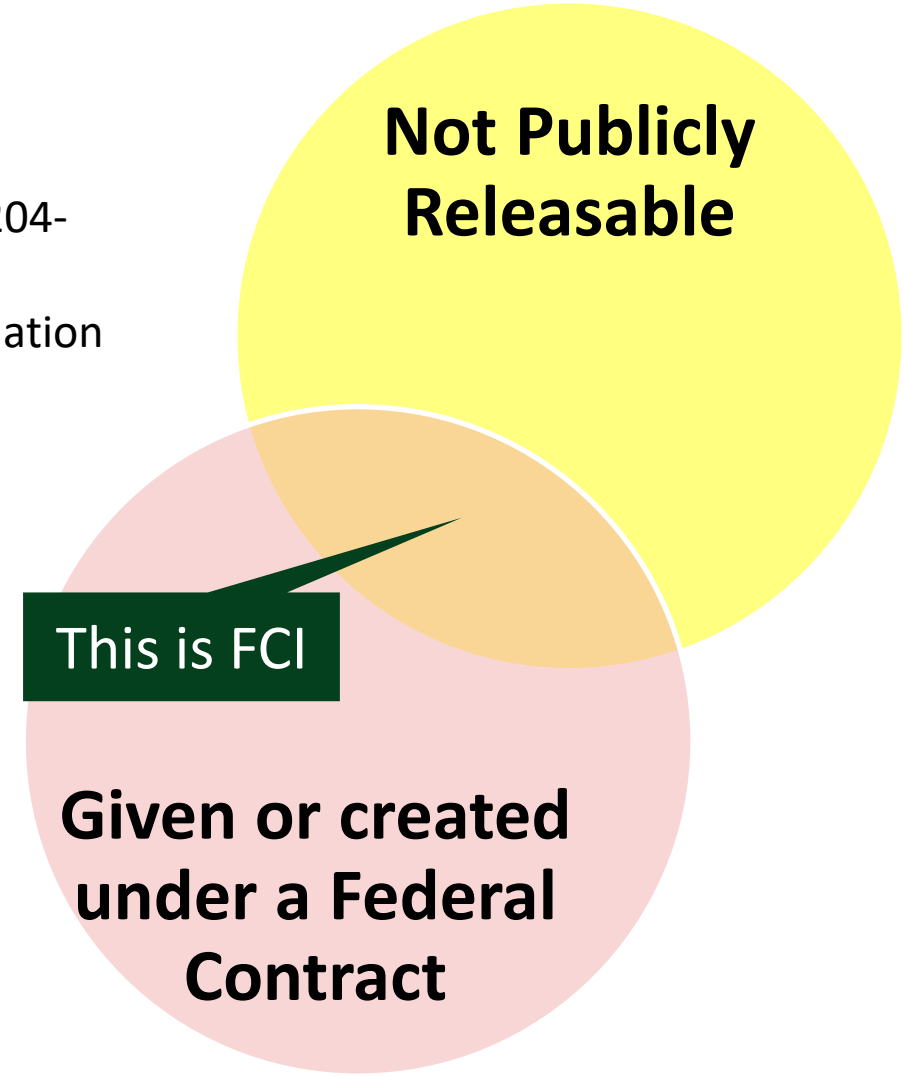
- **Protecting Federal Contracting Information (FCI)**
  - Understanding the Government's Intellectual Property Types: FCI
  - Cybersecurity Maturity Model Certification (CMMC) & Acquisition Clauses
  - FAR cybersecurity clause (FAR 52.204-21)
  - Your Requirements for FCI
  - Authorized C3PAO Hints for CMMC Level 1
- **Protecting Controlled Unclassified Information (CUI)**
  - Understanding the Government's Intellectual Property Types: CUI
  - Cybersecurity Maturity Model Certification (CMMC) & Acquisition Clauses
  - Defense Federal Acquisition Rule Supplement (DFARS) Clauses
  - Your Requirements for CUI
- **Impacts of Rulemaking**

PROTECTING FEDERAL CONTRACTING INFORMATION (FCI)

Understanding the Government's Intellectual Property Types: Federal Contract Information (FCI)

Federal Contract Information (FCI):

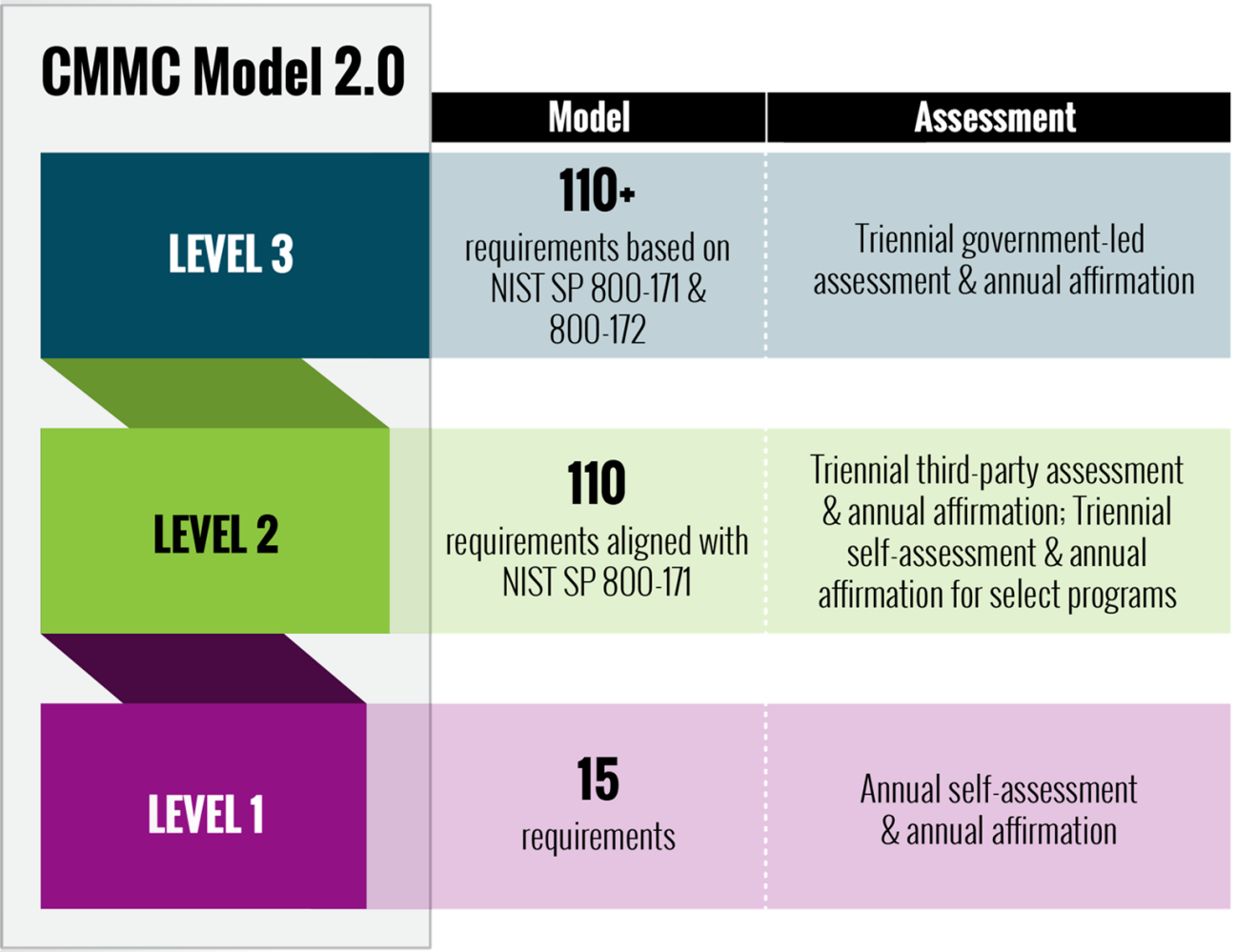
- Governed by 48 CFR § 52.204-21 - Basic Safeguarding of Covered Contractor Information Systems
- CMMC Info
  - *CMMC Level 1*
  - *15 Information Security Requirements*



Federal contract information means *information*, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including *information* provided by the Government to the public (such as on public websites) or simple transactional *information*, such as necessary to process payments.

Information means any communication or representation of knowledge such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual (Committee on National Security Systems Instruction (CNSSI) 4009).

CMMC Model 2.0 | Level 1



Federal Contracting Information (FCI) Only

48 CFR § 52.204-21 – Basic Safeguarding of Covered Contractor Information Systems

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

(b) Safeguarding requirements and procedures.

(1) The Contractor shall apply the following basic safeguarding requirements and procedures to protect covered contractor information systems. Requirements and procedures for basic safeguarding of covered contractor information systems shall include, at a minimum, the following security controls:

(i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

(ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

(iii) Verify and control/limit connections to and use of external information systems.

(iv) Control information posted or processed on publicly accessible information systems.

(v) Identify information system users, processes acting on behalf of users, or devices.

(vi) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

(vii) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.

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

(b) Safeguarding requirements and procedures.

(1) The Contractor shall apply the following basic safeguarding requirements and procedures to protect covered contractor information systems. Requirements and procedures for basic safeguarding of covered contractor information systems shall include, at a minimum, the following security controls:

…

(viii) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

(ix) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.

(x) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.

(xi) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

(xii) Identify, report, and correct information and information system flaws in a timely manner.

(xiii) Provide protection from malicious code at appropriate locations within organizational information systems.

(xiv) Update malicious code protection mechanisms when new releases are available.

(xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

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

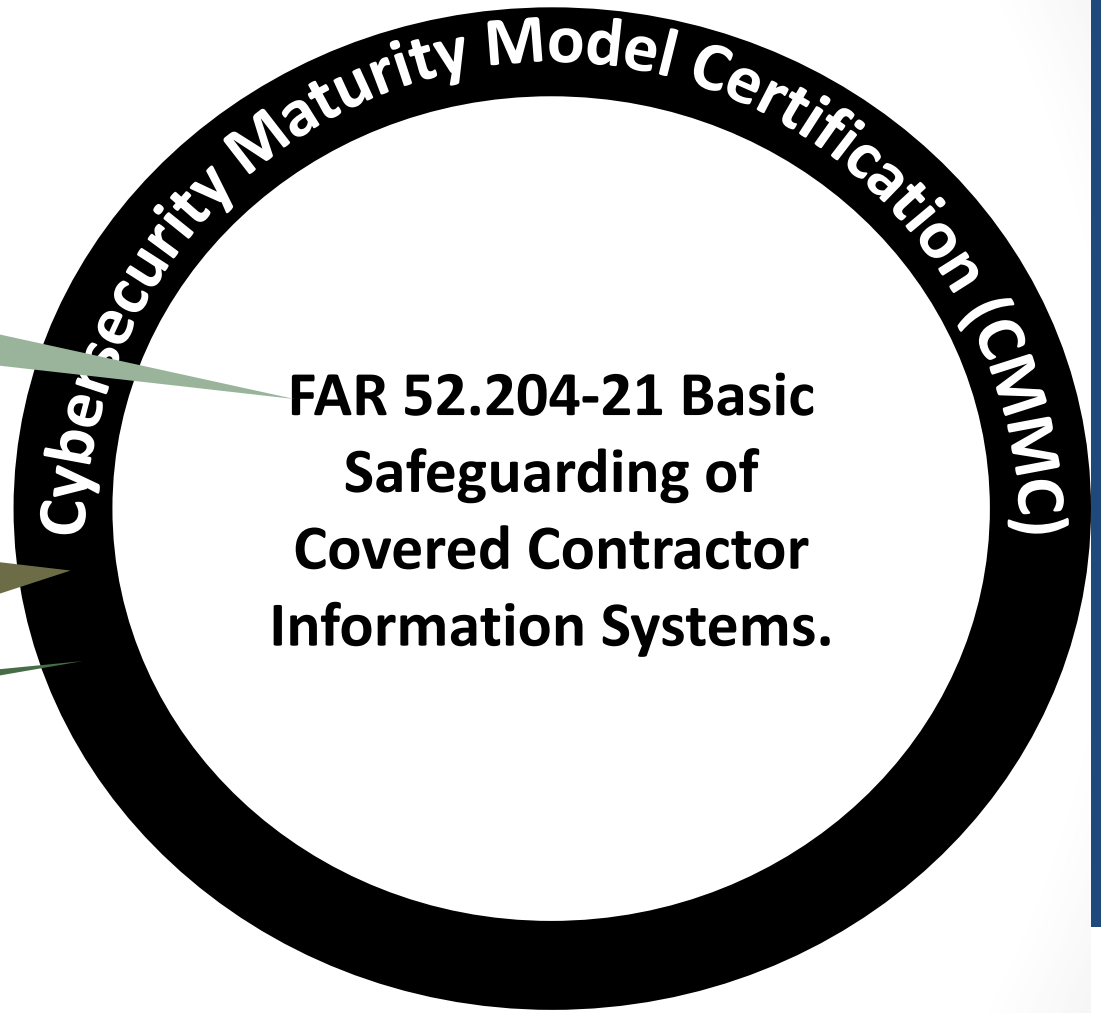
(b) Safeguarding requirements and procedures.

(2) Other requirements. This clause does not relieve the Contractor of any other specific safeguarding requirements specified by Federal agencies and departments relating to covered contractor information systems generally or other Federal safeguarding requirements for controlled unclassified information (CUI) as established by Executive Order 13556.

(c) Subcontracts. The Contractor shall include the substance of this clause, including this paragraph (c), in subcontracts under this contract (including subcontracts for the acquisition of commercial products or commercial services, other than commercially available off-the-shelf items), in which the subcontractor may have Federal contract information residing in or transiting through its information system.

Your Requirements for FCI

1. Implement FAR 52	FAR 52.204-21
2. Conduct Annual Self Assessment	Pending Rulemaking
3. Submit Self-Attestation[1]	Pending Rulemaking



Authorized C3PAO Hints for CMMC Level 1

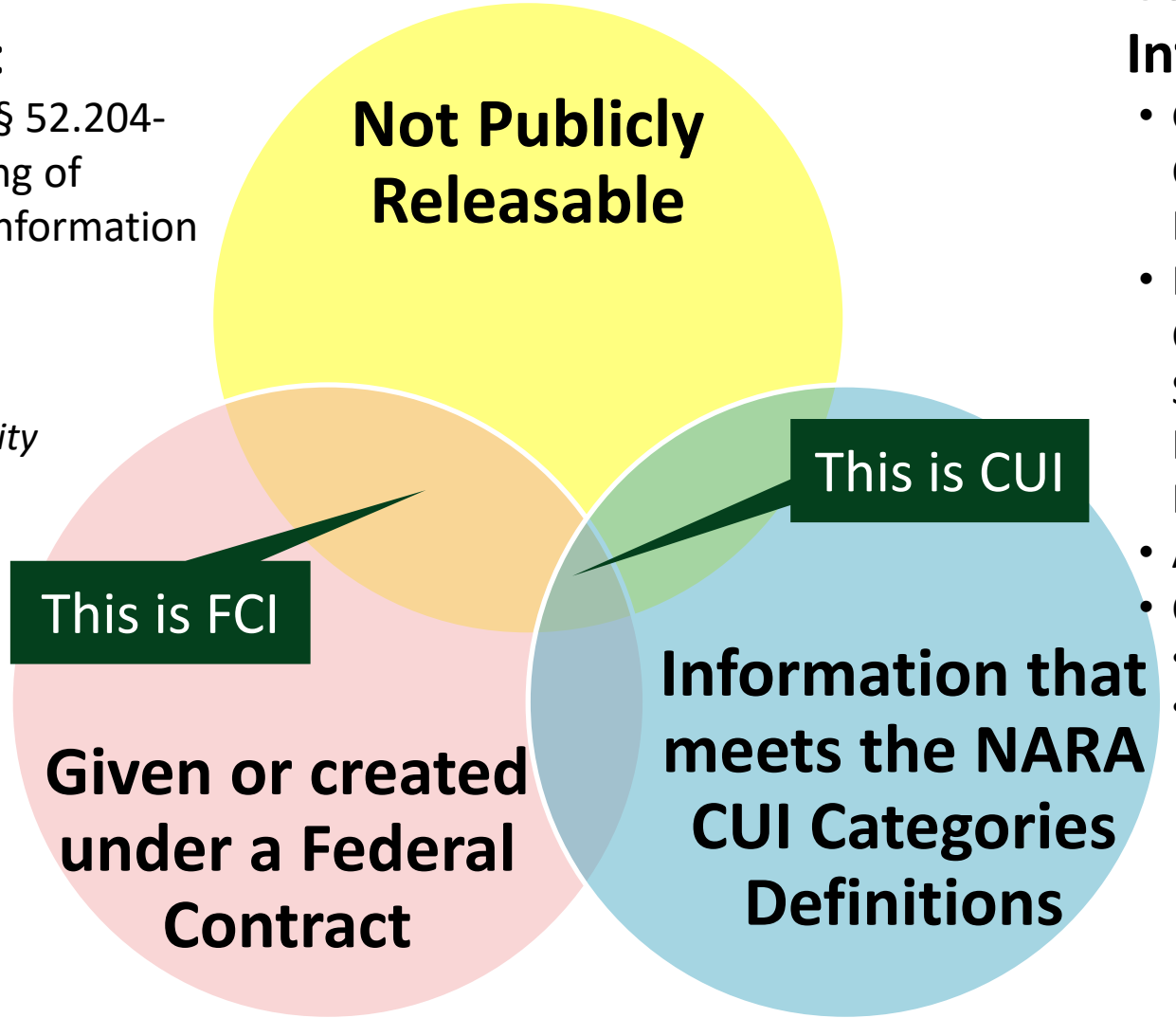
- **Use NIST SP 800-171 & NIST SP 800-171A to guide your implementation**
  - Likely legal references in a court of law
- **Have a System Security Plan**
  - Proves you are doing due diligence
- **Document your annual reviews in the your SSP**

PROTECTING CONTROLLED UNCLASSIFIED INFORMATION (CUI)

Understanding the Government's Intellectual Property Types

Federal Contract Information (FCI):

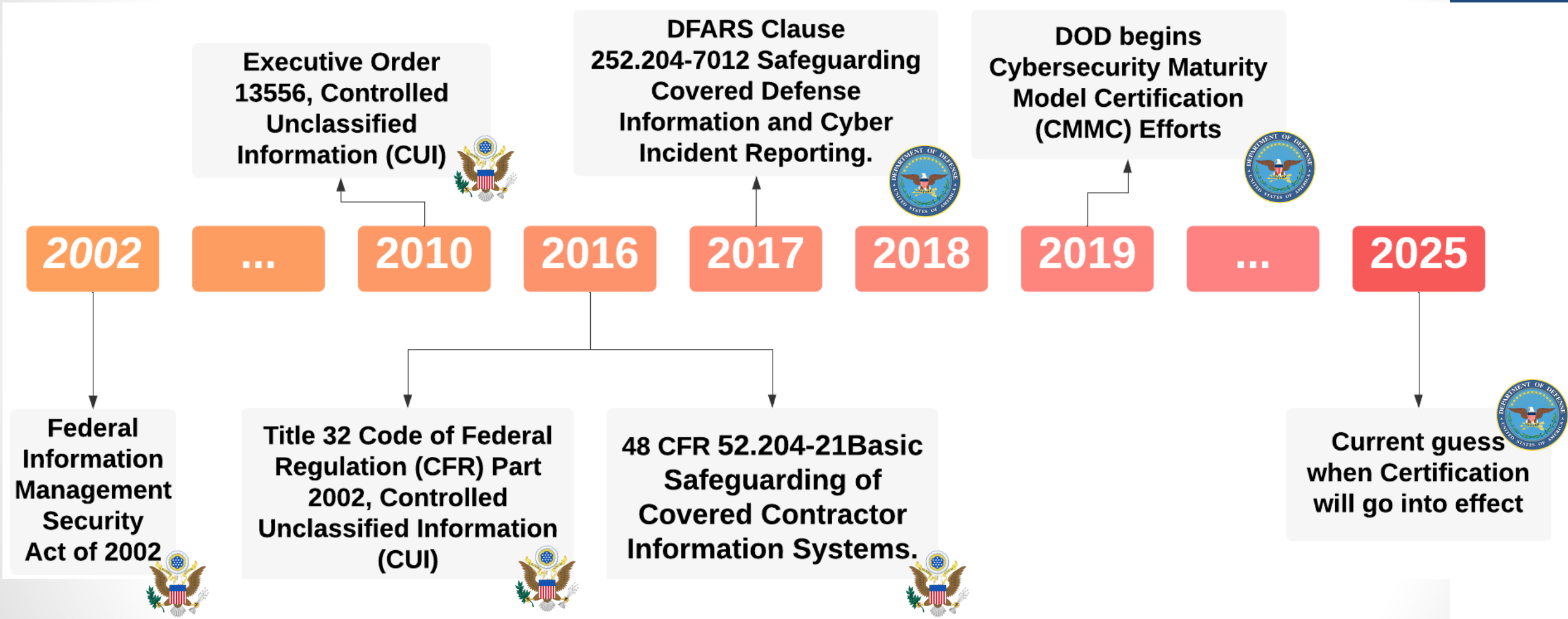
- Governed by 48 CFR § 52.204-21 - Basic Safeguarding of Covered Contractor Information Systems
- CMMC Info
  - *CMMC Level 1*
  - *15 Information Security Requirements*



Controlled Unclassified Information (CUI):

- Governed by 32 CFR Part 2002 - Controlled Unclassified Information (CUI)
- Primarily specified in DFARS Clause 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting
- All CUI is FCI by default
- CMMC Info
  - *CMMC Level 2*
  - *110 Information Security Requirements*

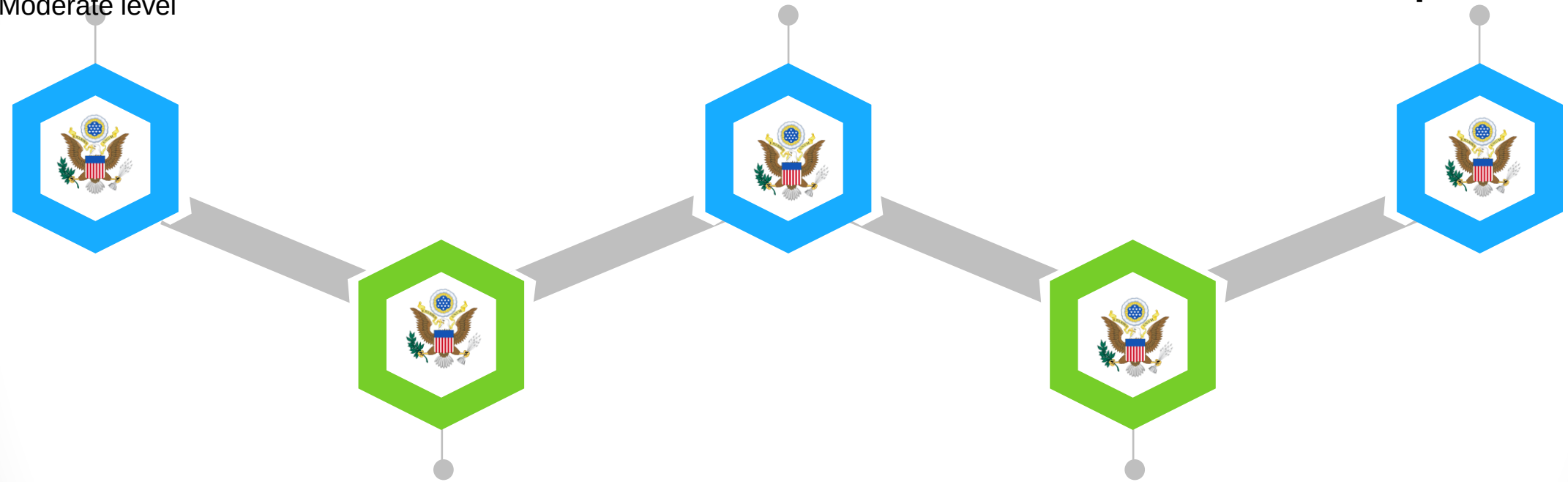
The Journey to 3rd Party Certification



The Journey to NIST SP 800-171

32 CFR Part 2002 Establishes:

- NIST SP 800-171 as the baseline
- CUI must be protected at no less than Moderate level



NIST SP 800-53 Moderate Security Baseline

NIST SP 800-37, Risk Management Framework

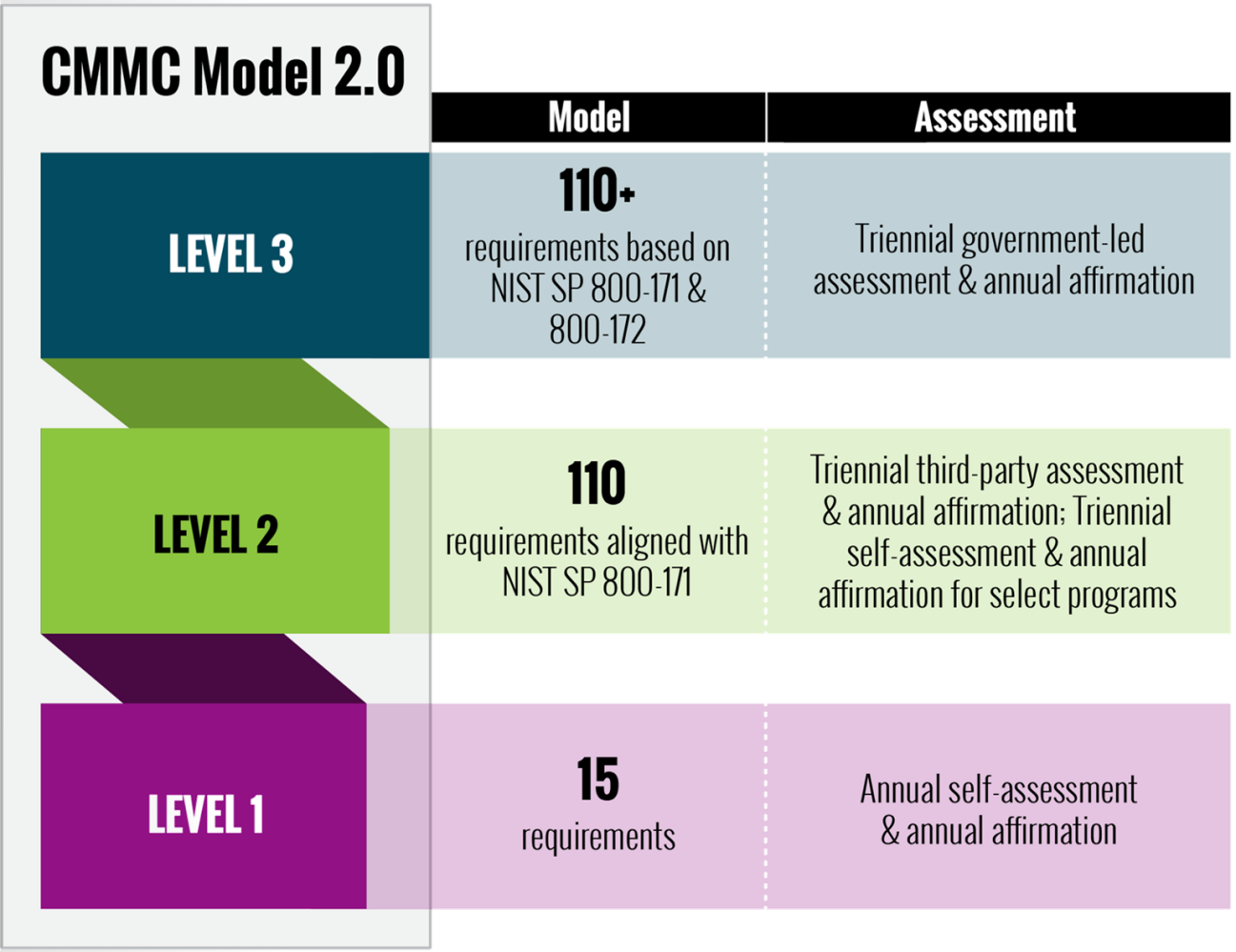
NIST SP 800-171 Appendix E, Tailoring Criteria

NIST SP 800-171 Security Requirements

NIST SP 800-171

- **NIST Special Publication 800-171 Revision 2, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations"**
  - "The purpose of this publication is to provide federal agencies with recommended security requirements for protecting the confidentiality of CUI:
    (1) when the CUI is resident in a nonfederal system and organization;
    (2) when the nonfederal organization is not collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency; and
    (3) where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category listed in the CUI Registry."

CMMC Model 2.0 | Level 2



Controlled Unclassified Information (CUI) + FCI

NIST SP 800-172 Rev 1

NIST SP 800-171 Rev 2

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

Federal Contracting Information (FCI) Only

48 CFR § 52.204-21 – Basic Safeguarding of Covered Contractor Information Systems

DFARS Clause 252.204-7008 Compliance with Safeguarding Covered Defense Information Controls.

(b) The security requirements required by contract clause 252.204-7012, shall be implemented for all covered defense information on all covered contractor information systems that support the performance of this contract.

(c) For covered contractor information systems that are not part of an information technology service or system operated on behalf of the Government (see 252.204-7012(b)(2)—

(1) By submission of this offer, the Offeror represents that it will implement the security requirements specified by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (see http://dx.doi.org/10.6028/NIST.SP.800-171) that are in effect at the time the solicitation is issued or as authorized by the contracting officer not later than December 31, 2017.

(2)(i) If the Offeror proposes to vary from any of the security requirements specified by NIST SP 800-171 that are in effect at the time the solicitation is issued or as authorized by the Contracting Officer, the Offeror shall submit to the Contracting Officer, for consideration by the DoD Chief Information Officer (CIO), a written explanation of—

(A) Why a particular security requirement is not applicable; or

(B) How an alternative but equally effective, security measure is used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection.

(ii) An authorized representative of the DoD CIO will adjudicate offeror requests to vary from NIST SP 800-171 requirements in writing prior to contract award. Any accepted variance from NIST SP 800-171 shall be incorporated into the resulting contract.

DFARS Clause 252.204-7012

"Adequate Security"

(b)(1)(ii) - No "skinnying" the requirements down to one system

(b)(2)(i) – NIST SP 800-171 Compliance driver

(b)(2)(ii)(A) – 30 days to implement upon contract award

(b)(2)(ii)(B) – ONLY the DoD CIO or designee can approve deviations from NIST SP 800-171

DFARS 252.204-7012 (b) Adequate security.:

The Contractor shall provide adequate security on all covered contractor information systems. To provide adequate security, the Contractor shall implement, at a minimum, the following information security protections:

(1) For covered contractor information systems that are part of an Information Technology (IT) service or system operated on behalf of the Government, the following security requirements apply:

(i) Cloud computing services shall be subject to the security requirements specified in the clause 252.239-7010, Cloud Computing Services, of this contract.

(ii) Any other such IT service or system (i.e., other than cloud computing) shall be subject to the security requirements specified elsewhere in this contract.

(2) For covered contractor information systems that are not part of an IT service or system operated on behalf of the Government and therefore are not subject to the security requirement specified at paragraph (b)(1) of this clause, the following security requirements apply:

(i) Except as provided in paragraph (b)(2)(ii) of this clause, the covered contractor information system shall be subject to the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (available via the internet at http://dx.doi.org/10.6028/NIST.SP.800-171) in effect at the time the solicitation is issued or as authorized by the Contracting Officer.

(ii) (A) The Contractor shall implement NIST SP 800-171, as soon as practical, but not later than December 31, 2017. For all contracts awarded prior to October 1, 2017, the Contractor shall notify the DoD Chief Information Officer (CIO), via email at osd.dibcsia@mail.mil, within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award.

(B) The Contractor shall submit requests to vary from NIST SP 800-171 in writing to the Contracting Officer, for consideration by the DoD CIO. The Contractor need not implement any security requirement adjudicated by an authorized representative of the DoD CIO to be nonapplicable or to have an alternative, but equally effective, security measure that may be implemented in its place.

(C) If the DoD CIO has previously adjudicated the contractor's requests indicating that a requirement is not applicable or that an alternative security measure is equally effective, a copy of that approval shall be provided to the Contracting Officer when requesting its recognition under this contract.

DFARS Clause 252.204-7012 & Supply Chain Compliance:

Cloud Service Provider Compliance

Cloud Service Providers must be FedRAMP Moderate or equivalent compliant

Cloud Service Providers must comply with paras a to g of this clause

DFARS 252.204-7012 (b) Adequate security.(2)(ii)(D):

"If the contractor intends to use an external cloud service provider to store, process, or transmit any covered defense information in performance of this contract, the Contractor shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline (https://www.fedramp.gov/resources/documents/) and that the cloud service provider complies with requirements in paragraphs (c) through (g) of this clause for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment."

DFARS Clause 252.204-7012

"Cyber incident reporting "

(c)(1)(ii) – Key word here is "affects" in its most general sense

(a) "Rapidly report" means within 72 hours of discovery of any cyber incident.

(c)(3) – Don't wait until you have an incident. DIBNet will accept e-mailed reports

(d) – Don't delete malware when discovered

(e) – Get media cloning hardware/software

(f) & (g) – DoD has the right to all the info as they want

(c) Cyber incident reporting requirement.

(1) When the Contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support and identified in the contract, the Contractor shall—

(i) Conduct a review for evidence of compromise of covered defense information, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered contractor information system(s) that were part of the cyber incident, as well as other information systems on the Contractor's network(s), that may have been accessed as a result of the incident in order to identify compromised covered defense information, or that affect the Contractor's ability to provide operationally critical support; and

(ii) Rapidly report cyber incidents to DoD at http://dibnet.dod.mil.

(2) Cyber incident report. The cyber incident report shall be treated as information created by or for DoD and shall include, at a minimum, the required elements at http://dibnet.dod.mil.

(3) Medium assurance certificate requirement. In order to report cyber incidents in accordance with this clause, the Contractor or subcontractor shall have or acquire a DoD-approved medium assurance certificate to report cyber incidents. For information on obtaining a DoD-approved medium assurance certificate, see http://iase.disa.mil/pki/eca/Pages/index.aspx.

(d) Malicious software. When the Contractor or subcontractors discover and isolate malicious software in connection with a reported cyber incident, submit the malicious software to DoD Cyber Crime Center (DC3) in accordance with instructions provided by DC3 or the Contracting Officer. Do not send the malicious software to the Contracting Officer.

(e) Media preservation and protection. When a Contractor discovers a cyber incident has occurred, the Contractor shall preserve and protect images of all known affected information systems identified in paragraph (c)(1)(i) of this clause and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow DoD to request the media or decline interest.

(f) Access to additional information or equipment necessary for forensic analysis. Upon request by DoD, the Contractor shall provide DoD with access to additional information or equipment that is necessary to conduct a forensic analysis.

(g) Cyber incident damage assessment activities. If DoD elects to conduct a damage assessment, the Contracting Officer will request that the Contractor provide all of the damage assessment information gathered in accordance with paragraph (e) of this clause.

DFARS Clause 252.204-7012 & Supply Chain Compliance

DFARS Flowdown Requirement

Contactors must include the entire clause in all sub-contracts

"for operationally critical support" means MSPs & anyone with elevated rights to systems with CUI

This is called "transferring risk." When in doubt, pass the clause down

Good luck getting an answer

IOTW, just because you are sub, you can't get out of any of the requirements

Let your partners know you have been hacked

(m) Subcontracts: The Contractor shall—

(1) Include this clause, including this paragraph (m), in subcontracts, or similar contractual instruments, for operationally critical support, or for which subcontract performance will involve covered defense information, including subcontracts for commercial items, without alteration, except to identify the parties. The Contractor shall determine if the information required for subcontractor performance retains its identity as covered defense information and will require protection under this clause, and, if necessary, consult with the Contracting Officer; and

(2) Require subcontractors to—

(i) Notify the prime Contractor (or next higher-tier subcontractor) when submitting a request to vary from a NIST SP 800-171 security requirement to the Contracting Officer, in accordance with paragraph (b)(2)(ii)(B) of this clause; and

(ii) Provide the incident report number, automatically assigned by DoD, to the prime Contractor (or next higher-tier subcontractor) as soon as practicable, when reporting a cyber incident to DoD as required in paragraph (c) of this clause.

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

- **Requirement:**
  - In order to be considered for award, if the Offeror is required to implement NIST SP 800-171, the Offeror shall have a current assessment (i.e., not more than 3 years old unless a lesser time is specified in the solicitation) (see 252.204-7020) for each covered contractor information system that is relevant to the offer, contract, task order, or delivery order. The Basic, Medium, and High NIST SP 800-171 DoD Assessments are described in the NIST SP 800-171 DoD Assessment Methodology located at https://www.acq.osd.mil/dpap/pdi/cyber/strategically_assessing_contractor_implementation_of_NIST_SP_800-171.html.
- **Assessment Types:**
  - Basic: Self-attested and posted to the Supplier Performance Risk System (SPRS)
  - Medium: Defense Contract Management Agency (DCMA) led paper-based assessment of the contractor
  - High: DCMA led on-premise or virtual validation of all NIST SP 800-171 requirements. Almost a DoD led CMMC Assessment
- **Contractual Flowdown Requirement**
  - None

252.204-7020 NIST SP 800-171 DoD Assessment Requirements

- **Requirement**
  - The Contractor shall provide access to its facilities, systems, and personnel necessary for the Government to conduct a Medium or High NIST SP 800-171 DoD Assessment, as described in NIST SP 800-171 DoD Assessment Methodology at https://www.acq.osd.mil/dpap/pdi/cyber/strategically_assessing_contractor_implementation_of_NIST_SP_800-171.html, if necessary.
- **The DoD now has rights to access and review any system containing CUI**
- **Mandates flowdown to Suppliers**
  - Require them to submit to SPRS

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

Contactors must include the entire clause in all sub-contracts

Contractor is required to validate NIST SP 800-171 implementation prior to award

Mandate your contractors to submit a SPRS entry and provide proof

(g) Subcontracts.

(1) The Contractor shall insert the substance of this clause, including this paragraph (g), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial products or commercial services (excluding commercially available off-the-shelf items).

(2) The Contractor shall not award a subcontract or other contractual instrument, that is subject to the implementation of NIST SP 800-171 security requirements, in accordance with DFARS clause 252.204-7012 of this contract, unless the subcontractor has completed, within the last 3 years, at least a Basic NIST SP 800-171 DoD Assessment, as described in https://www.acq.osd.mil/asda/dpc/cp/cyber/safeguarding.html#nistSP800171, for all covered contractor information systems relevant to its offer that are not part of an information technology service or system operated on behalf of the Government.

(3) If a subcontractor does not have summary level scores of a current NIST SP 800-171 DoD Assessment (i.e., not more than 3 years old unless a lesser time is specified in the solicitation) posted in SPRS, the subcontractor may conduct and submit a Basic Assessment, in accordance with the NIST SP 800-171 DoD Assessment Methodology, to webptsmh@navy.mil for posting to SPRS along with the information required by paragraph (d) of this clause.

252.204-7021 Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirement

- **Requirement**
  - (b) Requirements. The Contractor shall have a current (i.e. not older than 3 years) CMMC certificate at the CMMC level required by this contract and maintain the CMMC certificate at the required level for the duration of the contract.
  - (c) Subcontracts. The Contractor shall—
    - (1) Insert the substance of this clause, including this paragraph (c), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items, excluding commercially available off-the-shelf items; and
    - (2) Prior to awarding to a subcontractor, ensure that the subcontractor has a current (i.e., not older than 3 years) CMMC certificate at the CMMC level that is appropriate for the information that is being flowed down to the subcontractor.

DFARS Clause 252.204-7024 Notice on the Use of the Supplier Performance Risk System.

(b) The Supplier Performance Risk System (SPRS), available at https://piee.eb.mil/, will be used in the evaluation of the Quoter or Offeror's performance. SPRS retrieves item, price, quality, delivery, and contractor information on contracts from Government reporting systems in order to develop risk assessments.

(c) The Contracting Officer will consider SPRS risk assessments during the evaluation of quotations or offers received in response to this solicitation as follows:

(1) Item risk will be considered to determine whether the procurement represents a high performance risk to the Government.

(2) Price risk will be considered in determining if a proposed price is consistent with historical prices paid for a product or a service or otherwise creates a risk to the Government.

(3) Supplier risk, including but not limited to quality and delivery, will be considered to assess the risk of unsuccessful performance and supply chain risk.

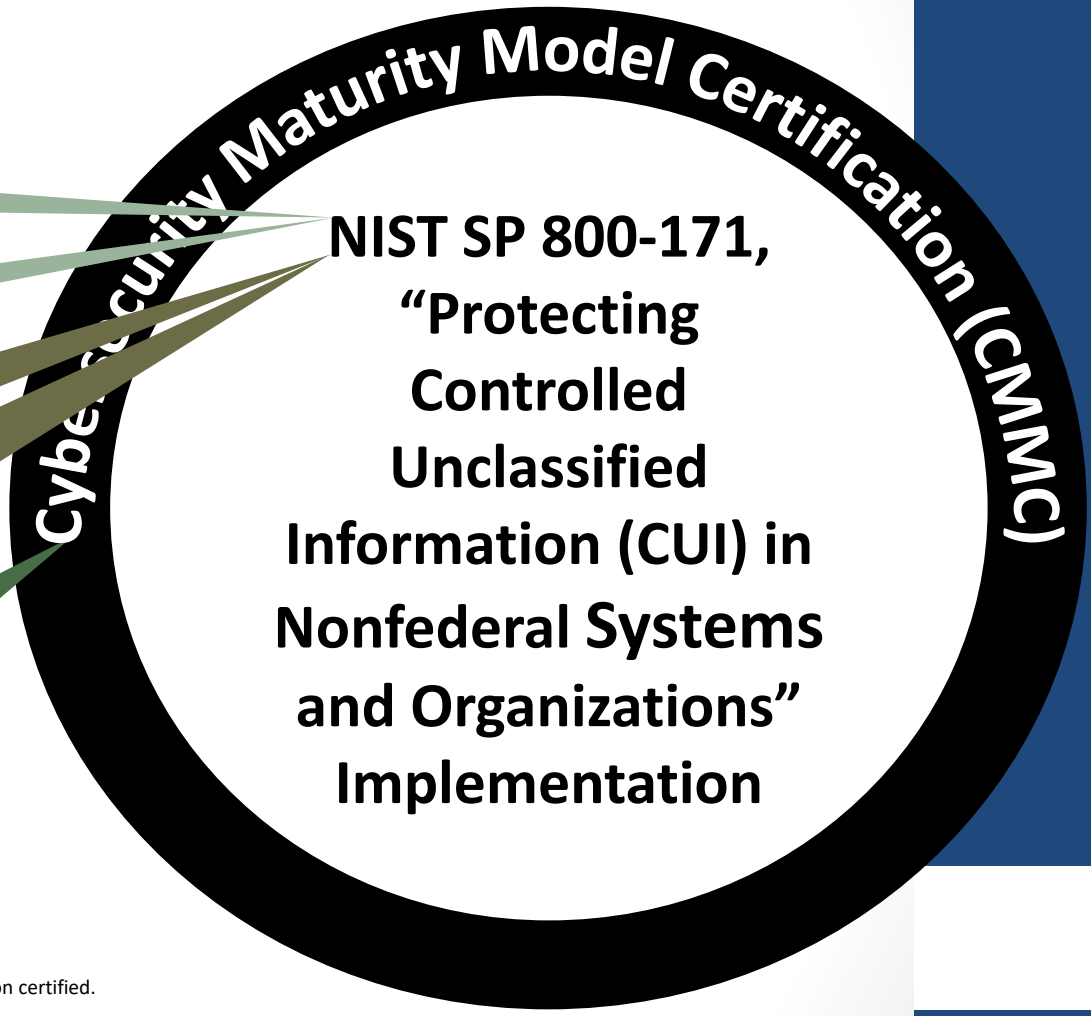
(d) SPRS risk assessments are generated daily. Quoters or Offerors are able to access their risk assessments by following the access instructions in the SPRS user's guide available at https://www.sprs.csd.disa.mil/reference.htm. Quoters and Offerors are granted access to SPRS for their own risk assessment classifications only. SPRS reporting procedures and risk assessment methodology are detailed in the SPRS user's guide. The method to challenge a rating generated by SPRS is also provided in the user's guide. SPRS evaluation criteria are available at https://www.sprs.csd.disa.mil/pdf/SPRS_DataEvaluationCriteria.pdf.

(e) The Contracting Officer may consider any other available and relevant information when evaluating a quotation or an offer.

Your Requirements for CUI

STEP: ***DO NOT DO THIS BACKWARDS!!!***

1. Implement NIST SP 800-171 per para 1.1	DFARS Clause 252.204-7008
	DFARS Clause 252.204-7012
2. Report On Your NIST SP 800-171 Implementation	DFARS Clause 252.204-7019
	DFARS Clause 252.204-7020
3. Get CMMC "Certified" [1]	DFARS Clause 252.204-7021[2]



Notes:

1. Organization are not required to implement CMMC. They are required to implement NIST SP 800-171 and eventually have their NIST SP 800-171 implementation certified.
2. DFARS Clause 252.204-7021 is currently "on-hold" and this line is subject to publication of the next version of the CMMC Rule in 2023

IMPACTS OF RULEMAKING

CMMC 1.0 RuleMaking

- **DFARS Clauses**
  - 252.204-7019 Notice of NIST SP 800-171 DoD Assessment Requirements **[FINAL & Enforced]**
  - 252.204-7020 NIST SP 800-171 DoD Assessment **[FINAL & Enforced]**
  - 252.204-7021 Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirement **[On Hold]**

CMMC 2.0 Rulemaking

- **32 CFR Part 170 {New}, Cybersecurity Maturity Model Certification (CMMC) Program**
  - DOD is proposing to implement the Cybersecurity Maturity Model Certification (CMMC) Framework, to help assess a Defense Industrial Base (DIB) contractor's compliance with and implementation of cybersecurity requirements to safeguard Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) transiting non-federal systems and mitigate the threats posed by Advanced Persistent Threats--adversaries with sophisticated levels of expertise and significant resources.
- **DFARS Clause 252.204-7021 Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirement**

CMMC Timeline

- **32 CFR Part 170**
  - Expected to be released for comment September 2023
- **If Interim**
  - Rule goes into Effect upon close out of comment period
  - If so and if released on time, goes into effect December 2023/January 2024
  - Ramping up rollout
  - First really showing up in FY 25 contracts
- **In Proposed**
  - Must go through full rule review before going into effect
  - If so and if released on time, goes into effect ~ September 2024
  - Ramping up rollout
  - First showing up in FY 25 contracts but real rollout in FY26
- **Ramping Up Rollout**
  - DoD to limit the number of contracts with CMMC Clause in it for the first few years in order for the ecosystem to grow

Questions…

As the CMMC Churns

Matthew A. Titcombe, CISSP, CCA, CCP
cmmc.services@peakinfosec.us
https://peakinfosec.com
(727) 378-4167