Cybersecurity for Government Contractors in 2023: Data in the Cloud

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

- Surgeons General's Warning
- Questions
- The Requirements
- Scoping
- Data in the Cloud

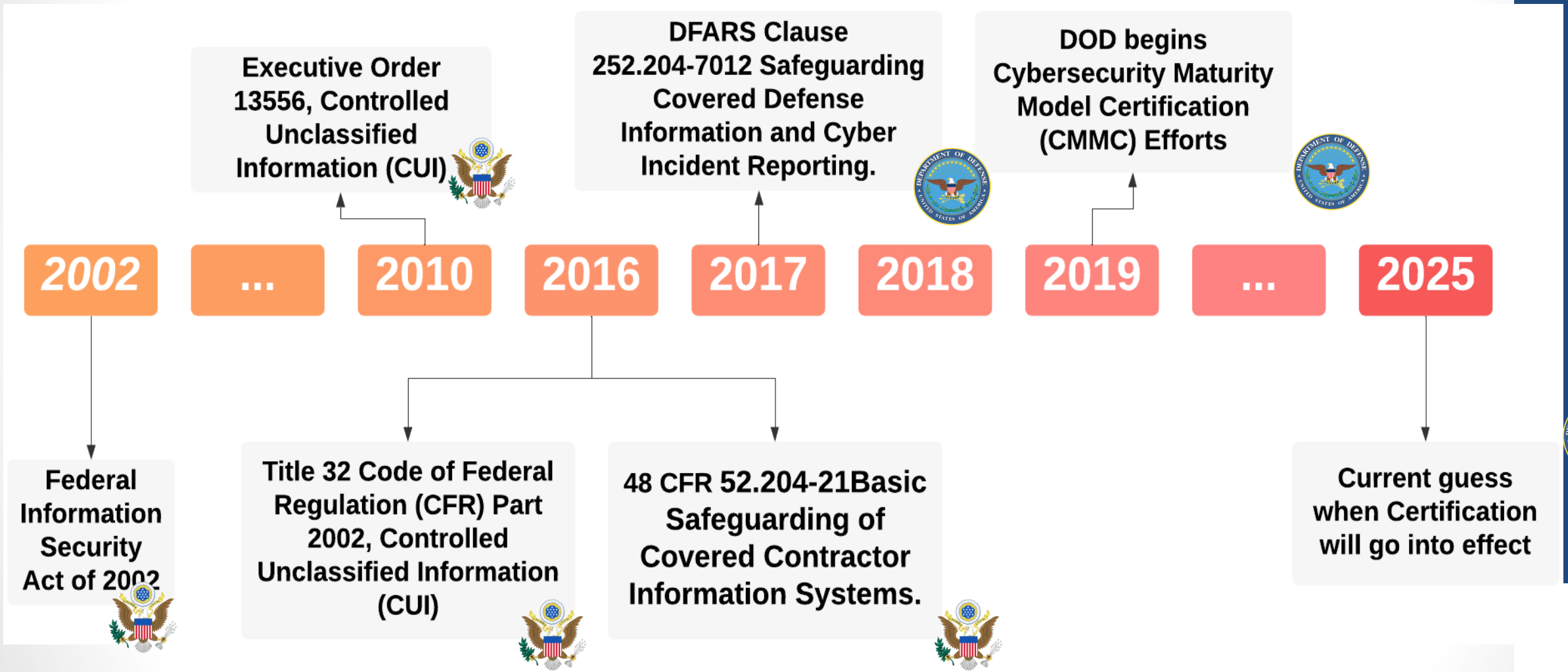
Surgeons General's Warning

- Discussing CMMC, NIST SP 800-171, FCI, & CUI have been proven to cause:
  - Anger
  - Anxiety
  - Brain Freezes
  - Confusion
  - Dumbfoundness
  - Mind-numbing pain
  - Panic-attacks
  - Sense of being overwhelmed

Questions…

The Requirements

The Journey to 3rd Party Certification



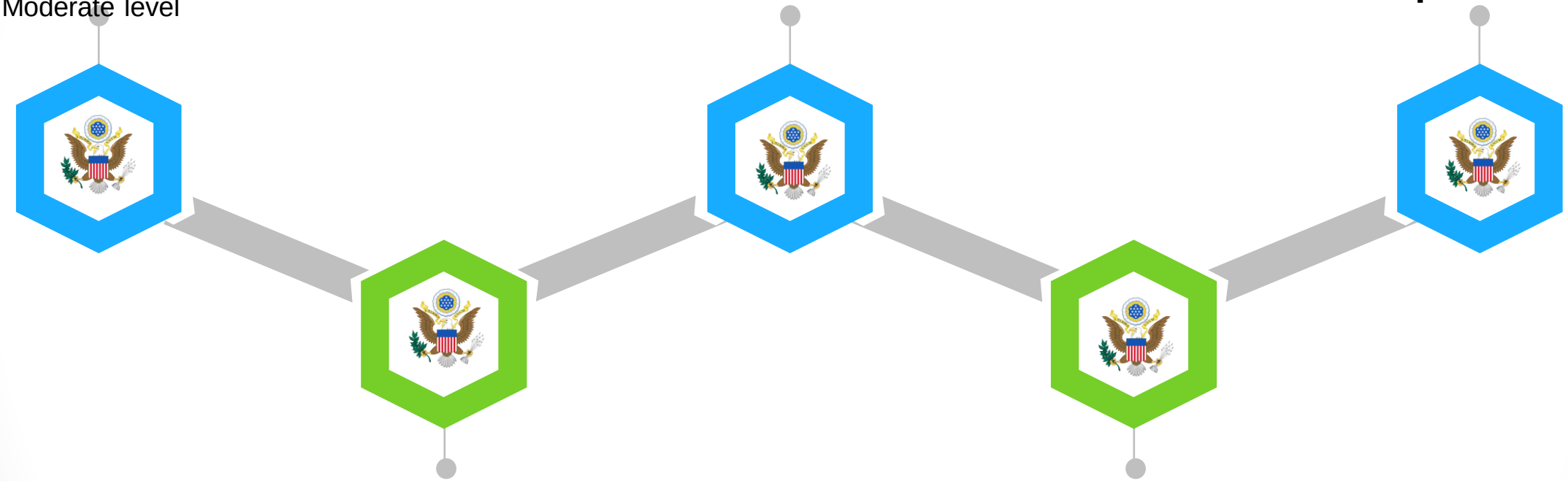
Moderate Baseline

- 32 CFR Part 2002, Controlled Unclassified Information (CUI)
  - § 2002.14(a)(3) “Agencies may increase CUI Basic's confidentiality impact level above moderate only internally, or by means of agreements”
  - § 2002.14(g) “CUI Basic is categorized at no less than the moderate confidentiality impact level”
  - § 2002.14(h)(2) “NIST SP 800-171 (incorporated by reference, see § 2002.2) defines the requirements necessary to protect CUI Basic on non-Federal information systems in accordance with the requirements of this part. Agencies must use NIST SP 800-171 when establishing security requirements to protect CUI's confidentiality on non-Federal information systems”

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

Federal Tailoring

Not all were worthy to Protect CUI

CUI

The CUI Basic Or Derived Security Requirement Is Reflected In And Is Traceable To The Security Control, Control Enhancement, Or Specific Elements Of The Control/Enhancement.

125 out of 262
48% of the Controls

NFO
"Non-Federal Organization"

Expected To Be Routinely Satisfied By Nonfederal Organizations Without Specification.

61 out of 262
23% of the Controls

NCO
"Not Confidentiality Oriented"

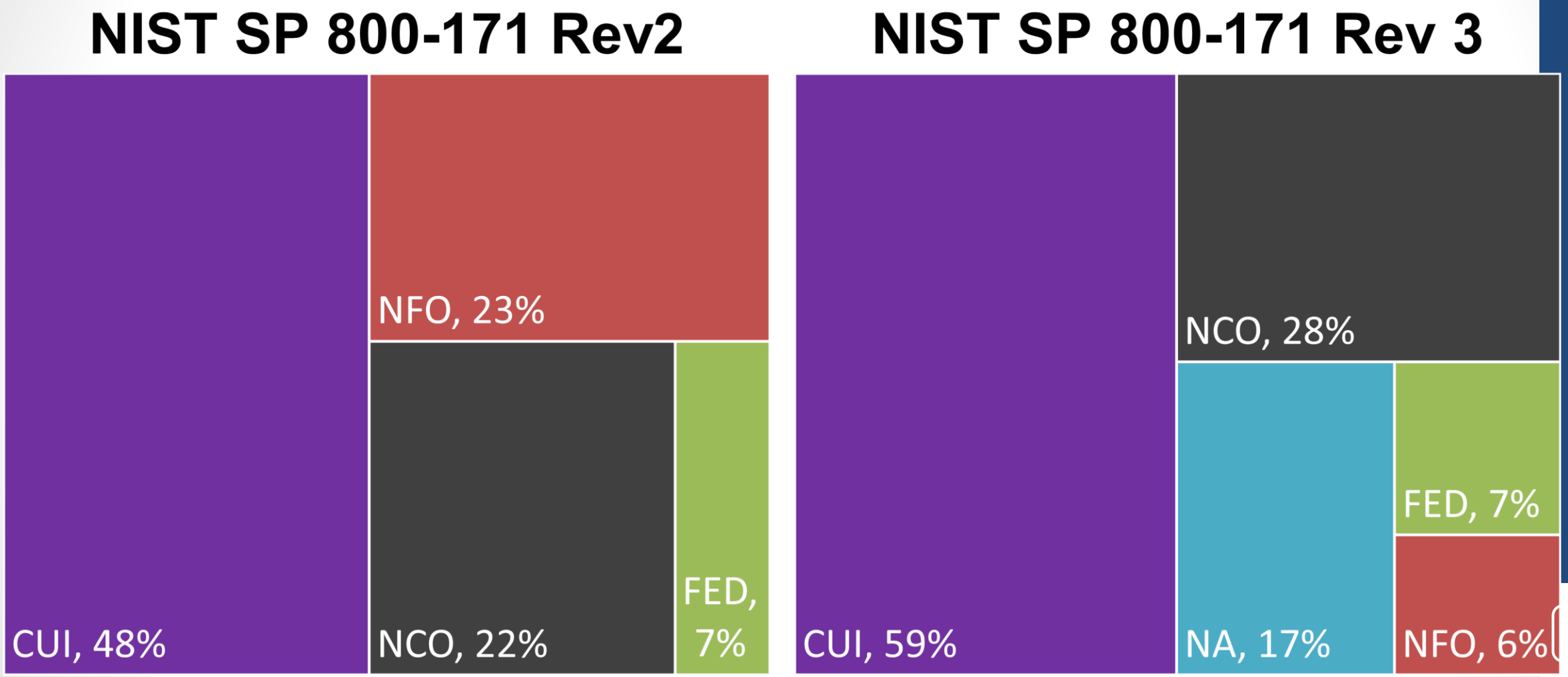
Not Directly Related To Protecting The Confidentiality Of CUI.

58 out of 262
22% of the Controls

FED

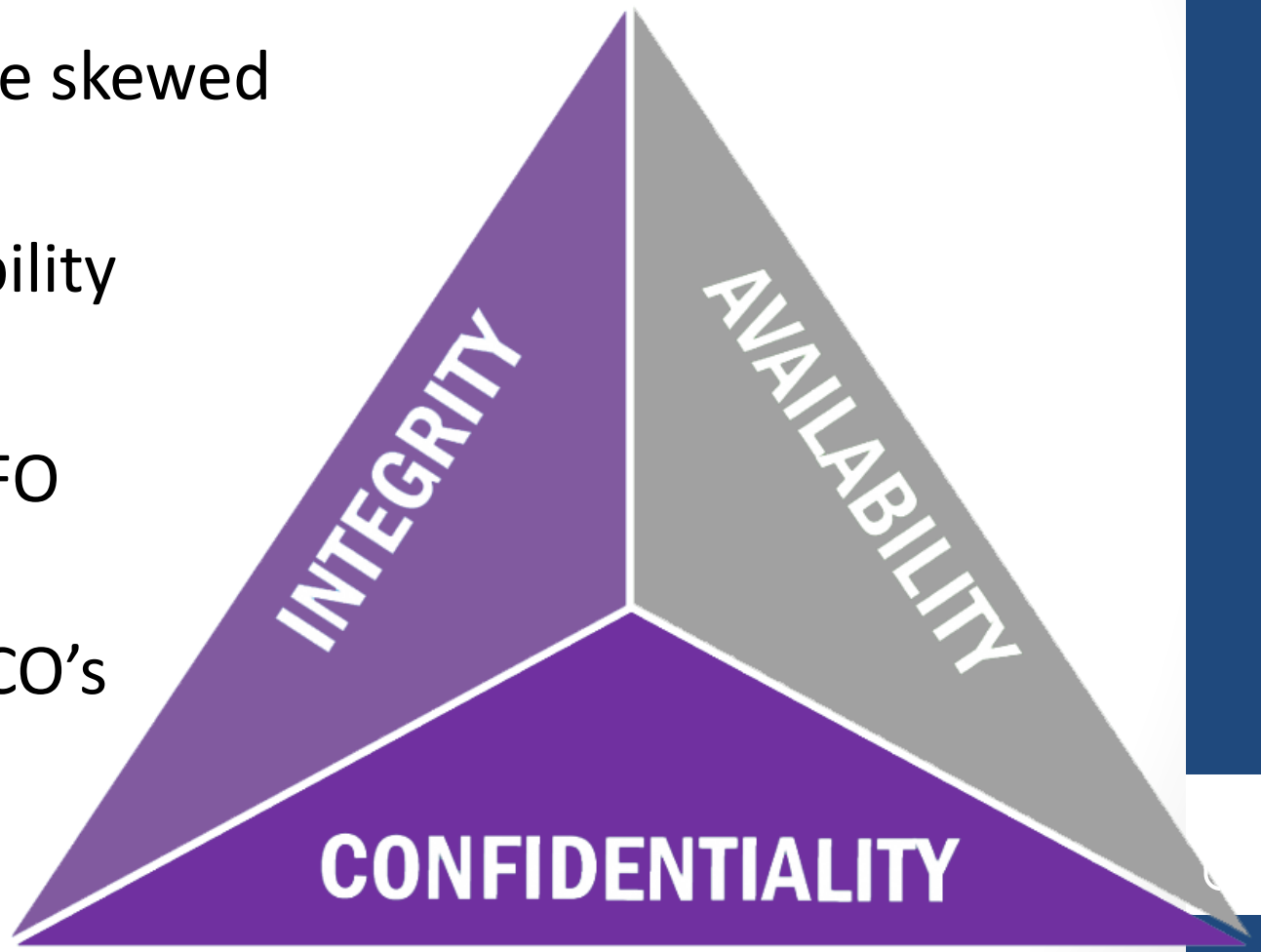
Uniquely Federal, Primarily The Responsibility Of The Federal Government.
18 out of 262
7% of the Controls

NIST SP 800-171 Rev 3 Tailoring



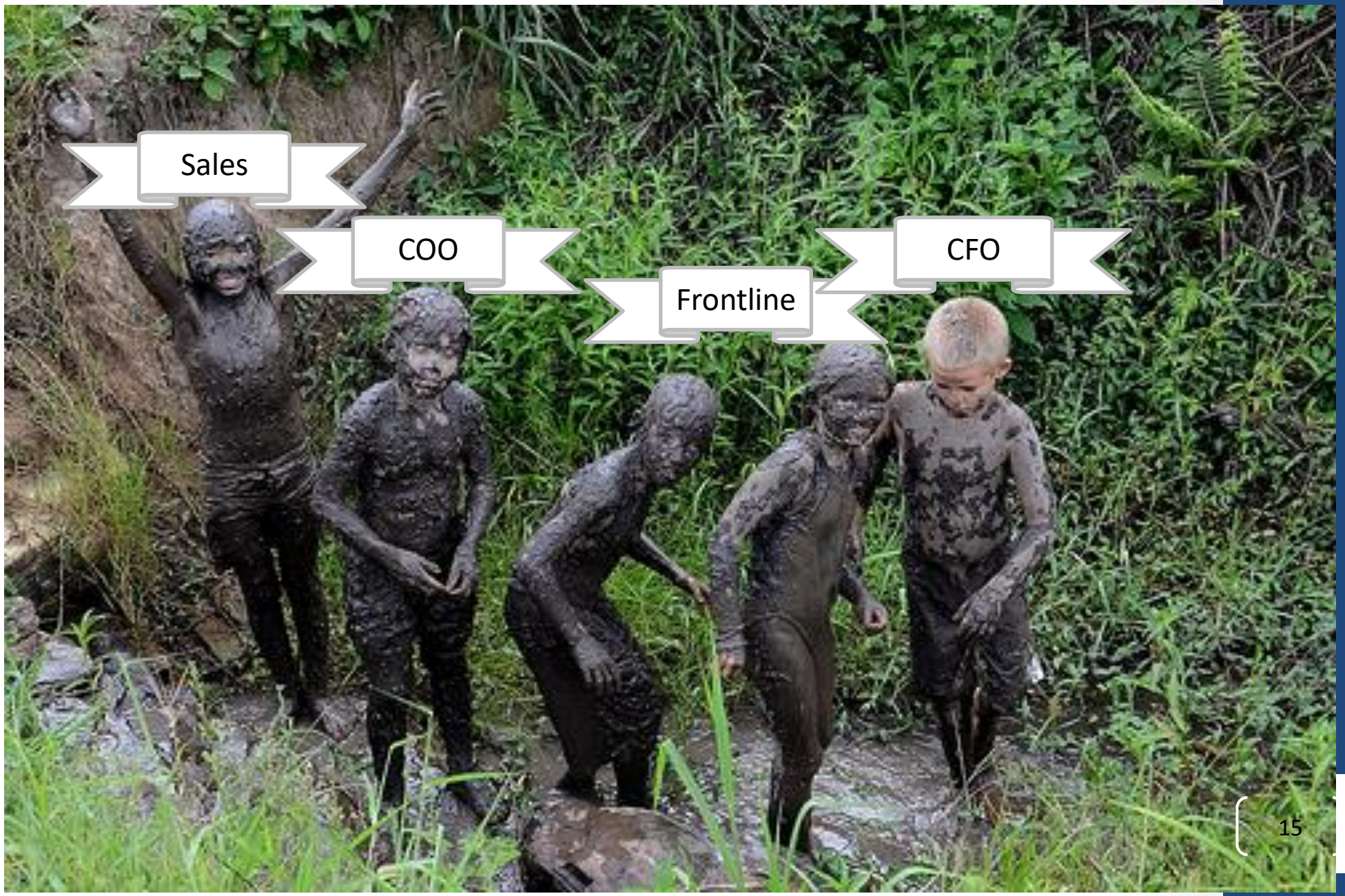
NIST SP 800-171 is Confidentiality & Integrity Centric

- NIST SP 800-171 was designed to be skewed towards Confidentiality
- NIST CSF is skewed towards Availability
- Skew Impacts:
  - Businesses need to implement NFO controls to be successful
  - Businesses need to implement NCO's to protect their business



Scoping

Protecting the DoD's IP via NIST SP 800-171 is Information Centric



Scope of Applicability

"The requirements apply to components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components."

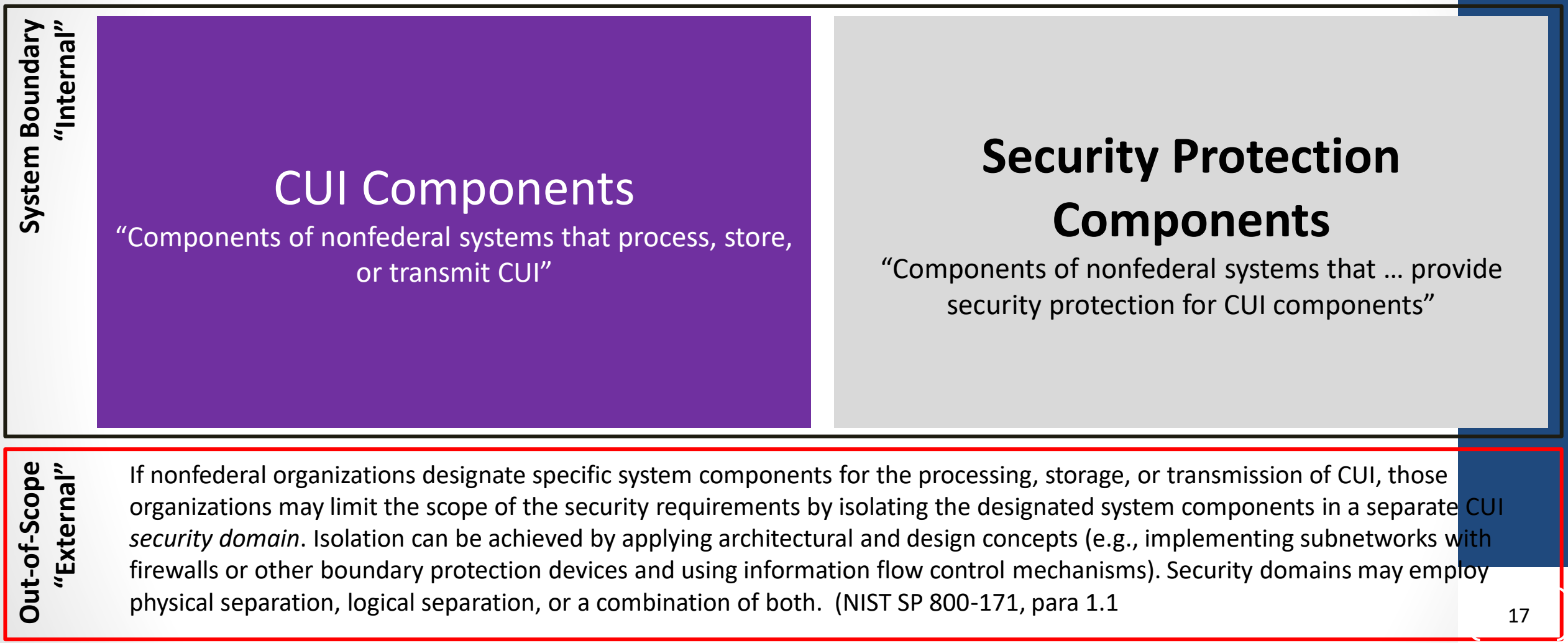
NIST SP 800-171, para 1.1

110 NIST SP 800-171 Requirements + 62 Non-Federal Organization (NFO) Controls

Applies to people, facilities, and technologies

Two types of components

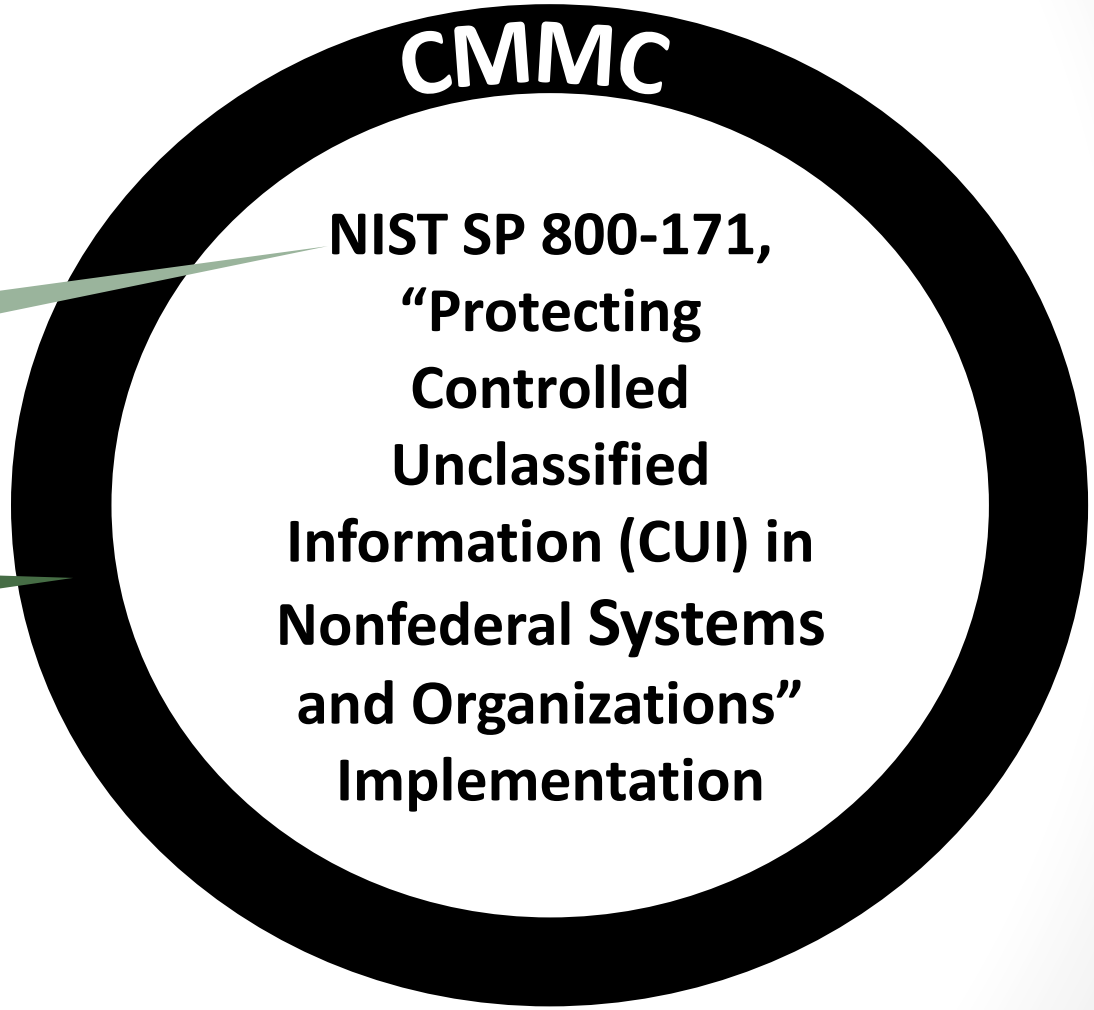
Scope of Applicability Diagram



What is Cybersecurity Maturity Model Certification (CMMC)?

DFARS -7012, para (b)(2)(ii)(A), implement NIST SP 800-171

CMMC is just 3rd Party Certification of your implementation



CMMC Assessment Scoping

Identifying the CMMC Assessment Scope

> "This document provides information on the categorization of assets that, in turn, inform the specification of assessment scope for a Cybersecurity Maturity Model Certification (CMMC) assessment. The ensuing sections discuss CMMC asset categories as well as the associated requirements for Defense Industrial Base (DIB) contractors and CMMC assessments."

CMMC Assessment Scope, Level 2, Version 2.0, As of December 2021, pg 1

This document provides information on the … specification of assessment scope for a Cybersecurity Maturity Model Certification (CMMC) assessment.

Establishes requirements for CMMC Assessments

Scope of Applicability Diagram
NIST SP 800-171 Para 1.1

System Boundary "Internal"

CUI Components

"Components of nonfederal systems that process, store, or transmit CUI"

CUI Assets

"Assets that process, store, or transmit CUI"

Contractor Risk Managed Assets

"Assets that can, but are not intended to, process, store, or transmit CUI because of security policy, procedures, and practices in place Assets are not required to be physically or logically separated from CUI assets"

Specialized Assets

"Assets that may or may not process, store, or transmit CUI. Assets include: government property, Internet of Things (IoT) devices, Operational Technology (OT), Restricted Information Systems, and Test Equipment"

Security Protection Components

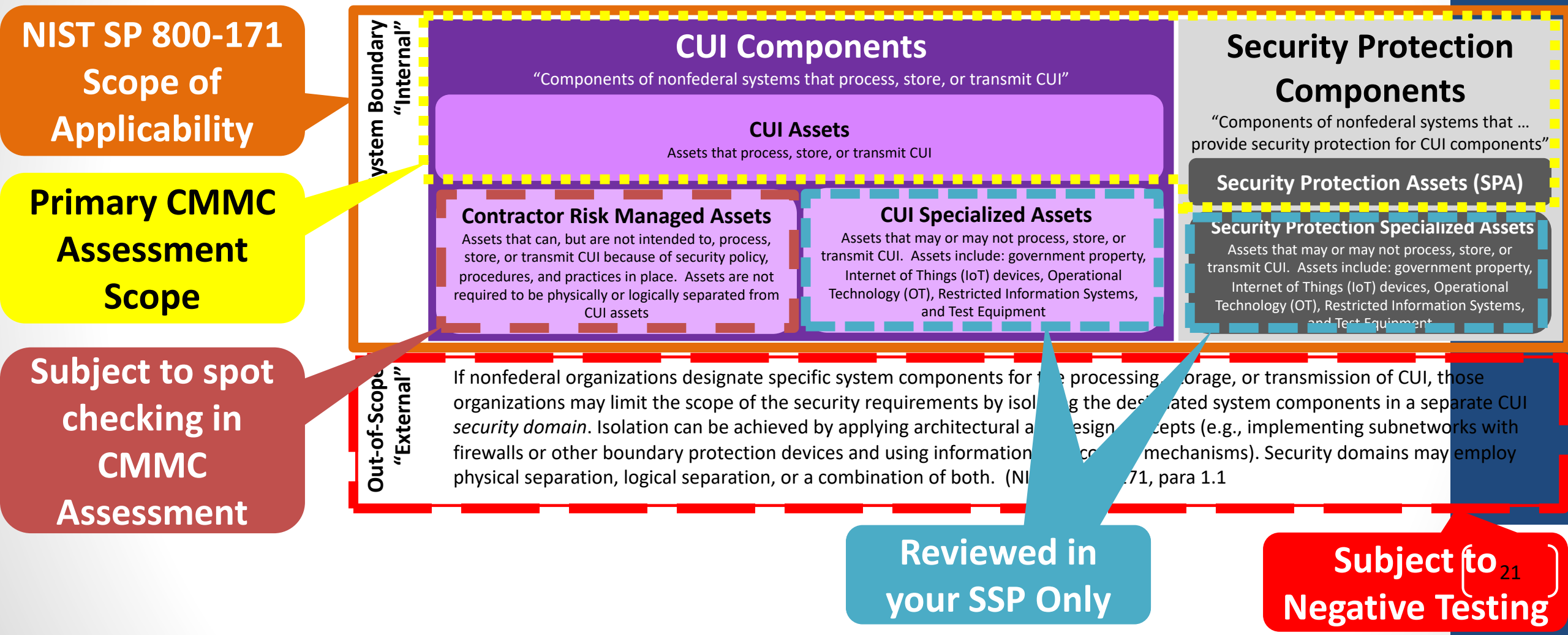
"Components of nonfederal systems that … provide security protection for CUI components"

A.K.A., Security Protection Assets in the CMMC Assessment Guide

Out-of-Scope "External"

If nonfederal organizations designate specific system components for the processing, storage, or transmission of CUI, those organizations may limit the scope of the security requirements by isolating the designated system components in a separate CUI *security domain*. Isolation can be achieved by applying architectural and design concepts (e.g., implementing subnetworks with firewalls or other boundary protection devices and using information flow control mechanisms). Security domains may employ physical separation, logical separation, or a combination of both. (NIST SP 800-171, para 1.1)

Scope of Applicability AND CMMC Assessment Scope

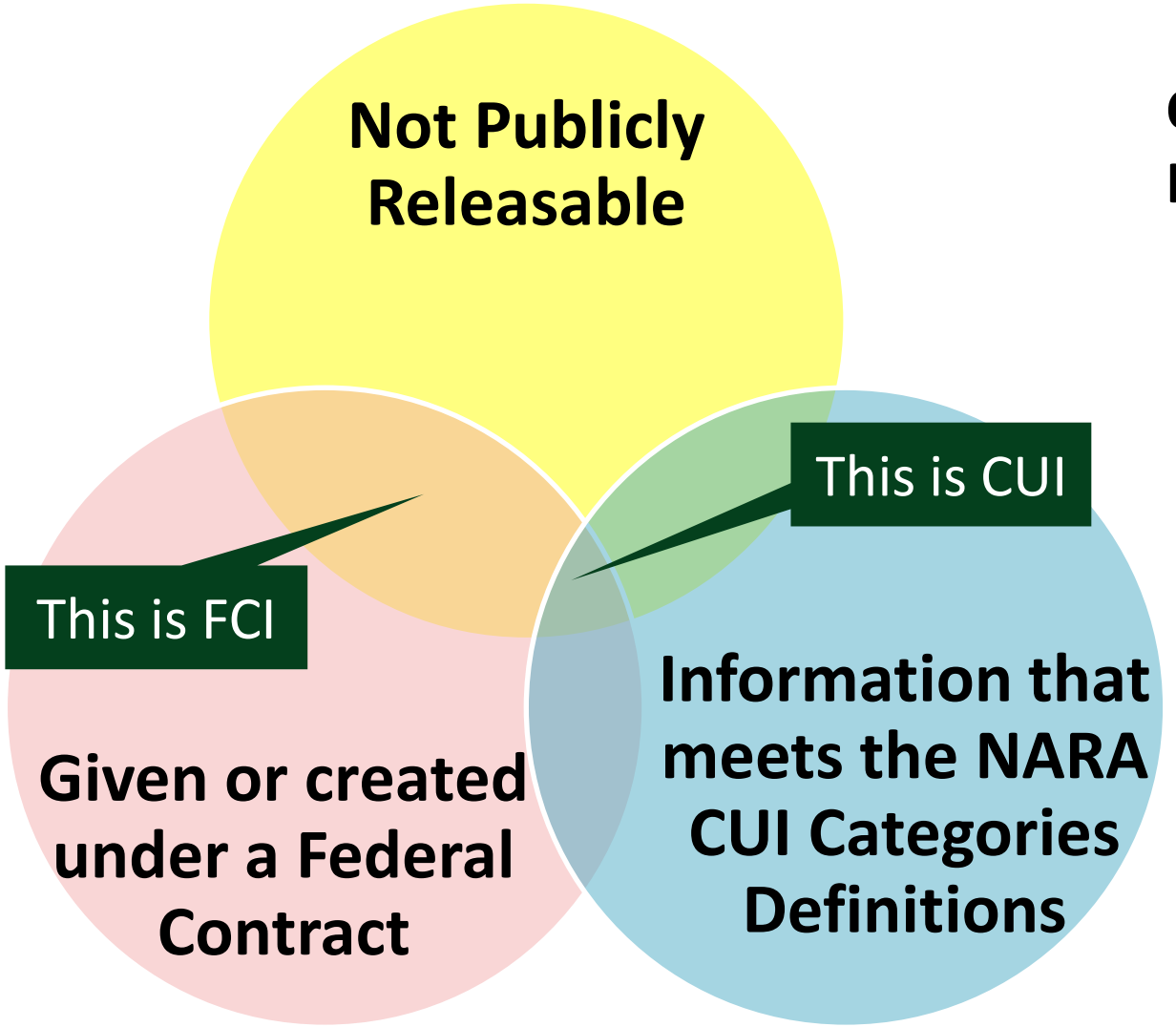


Data in the Cloud

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*
  - *17 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*

"CUI Basic" in the Cloud

- NIST SP 800-171 Revision 3 Initial public draft now includes "Cloud computing"

  All components must meet:

  - NIST SP 800-53 Revision 5 Moderate Baseline (c.f., NIST SP 800-53B);
  - NIST SP 800-171;
  - Or, FedRAMP Moderate

"The requirements apply to components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components."

NIST SP 800-171, para 1.1

DoD's CUI

ALL

DoD CUI, regardless of NARA Category is considered "Specified" for security protections

NARA's CUI Groups & Categories

- Critical Infrastructure
- Defense
  - ***Controlled Technical Information (CTI)***
  - DoD Critical Infrastructure Security Information
  - Naval Nuclear Propulsion Information
  - Unclassified Controlled Nuclear Information - Defense (USNI)
- Export Control
- *Financial*
- Intelligence
- *International Agreements*
- *Law Enforcement*
- *Legal*
- *Natural and Cultural Resources*
- *North Atlantic Treaty Organization (NATO)*
- *Nuclear*
- *Patents*
- *Privacy*
  - Personally Identifiable Information
  - Personal Health Information
  - Genomic data
- Procurement and Acquisition
- Proprietary Business Information
- Provisional
- *Statistical Tax*
- *Transportation*

Covered Defense Information per -7012

(a) “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 Governmentwide policies, and is—

(1) 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; or

(2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

Other NARA Categories Apply

Specified Security for CSPs

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

  "If the 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."

Export Controlled Information

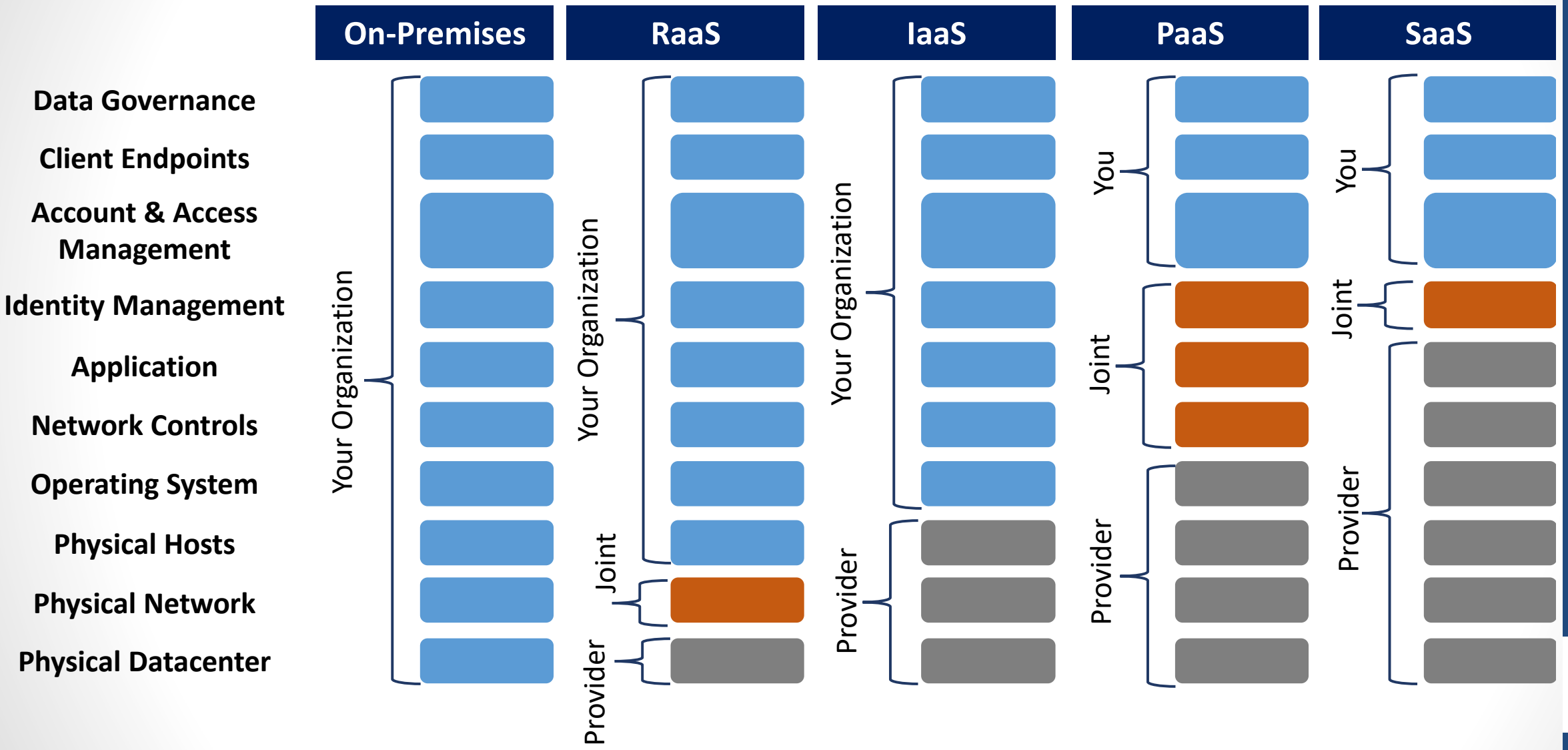
ALL

Export Controlled categories are considered “Specified” for security protections and requires a HIGH Security Baseline

Break Down by CUI Type

CUI Category/ Requirement	CUI Basic	DoD CUI	Export Controlled CUI with or with DoD CUI
CSP that stores, processes, or transmits CUI	NIST SP 800-53 Moderate NIST SP 800-171 FedRAMP Moderate	DFARS 252.204-7012 (b)(2)(ii)(D) compliant Provider	DFARS 252.204-7012 (b)(2)(ii)(D) compliant Provider **+** the provider must be a High Baseline
CUI CSP Commercial Example	Microsoft O365 configured to meet NIST SP 800-171	Microsoft O365 Government Community Cloud (GCC) configured to meet NIST SP 800-171	Microsoft O365 GCC-High (GCCH) configured to meet NIST SP 800-171
CSP that protects CUI	NIST SP 800-53 Moderate NIST SP 800-171 FedRAMP Moderate	NIST SP 800-53 Moderate NIST SP 800-171 FedRAMP Moderate	NIST SP 800-53 Moderate NIST SP 800-171 FedRAMP Moderate
CSP Commercial Example	Cisco DUO Federal or Commercial	Cisco DUO Federal or Commercial	Cisco DUO Federal or Commercial

Shared Services for Cloud



External Service Providers (ESP)

"A contractor can inherit practice objectives. A practice objective that is inherited is MET if adequate evidence is provided that the enterprise or another entity, such as an External Service Provider (ESP), performs the practice objective. An ESP may be external people, technology, or facilities that the contractor uses, including cloud service providers, managed service providers, managed security service providers, cybersecurity-as-a-service providers."

CMMC Level 2 Assessment Guide, pg 10

Also referenced as "Extending your IT"

DoD Cybersecurity FAQs for DFARS -7012

- Q7: Our Company has outsourced its IT support and systems to a third-party contractor. Are we still responsible for complying with DFARS clause 252.204-7012 and implementing NIST SP 800-171?
  - A7: Outsourcing your IT to another company does not transfer your DFARS clause 252.204-7012 responsibilities or implementation of NIST SP 800-171 requirements. Your company is responsible and accountable for meeting the contractual obligations with the Government as per the contract. The key to successfully demonstrating compliance with DFARS clause 252.204-7012 and NIST SP 800-171 is having a well written contract with the third-party that describes your requirements, and includes deliverables that meet or exceed requirements to protect DoD CUI. **If your IT service support is deemed to be less than or non-compliant with the contract, the company contracting with DoD is ultimately responsible.**

Inheritance versus Reciprocity

- **security control inheritance**
  - "A situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides."
- **reciprocity**
  - "Mutual agreement among participating organizations to accept each other's security assessments in order to reuse information system resources and/or to accept each other's assessed security posture in order to share information."

Inheritance versus Reciprocity Cont.

- For a CSP that is AICPA SOC II Type 2 Compliant, you can inherit applicable controls for the other security assessment
  - E.g., you can inherit the physical security controls for visitor management

You CANNOT claim the AICPA SOC II Type 2 meets

- NIST SP 800-53 Moderate
- NIST SP 800-171
- FedRAMP Moderate

Sanity Check

PUBLIC CONTRACTING INSTITUTE

Questions…

As the CMMC Churns

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