THE CYBER AB
CMMC CERTIFICATION
AUTHORIZED C3PAO

CAICO
CERTIFIED CMMC ASSESSOR

CAICO
CERTIFIED CMMC PROFESSIONAL

Scoping your FCI & CUI Environment

Matthew A. Titcombe, CISSP, CCA, CCP
CEO, Peak InfoSec

A Bit About Me

THE CYBER AB
CMMC CERTIFICATION
AUTHORIZED C3PAO

CAICO
CERTIFIED CMMC ASSESSOR

CAICO
CERTIFIED CMMC PROFESSIONAL

- **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

CMMC Implementation Myth Debunking

Defense Industrial Base (DIB) contractors are required to implement Cybersecurity Maturity Model Certification (CMMC)*

MYTH

* All of this is subject to change when the new CMMC Rule is published

The Facts: DFARS Clauses

- Clauses requiring implementation of NIST SP 800-171
  - DFARS Clause 252.204-7008 Compliance with Safeguarding Covered Defense Information Controls.

    (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.
  - DFARS Clause 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting
    - (b)(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.

The Facts: DFARS Clauses Cont.

- Clauses requiring reporting of NIST SP 800-171 implementation
  - DFARS Clause 252.204-7019, Notice of NIST SP 800-171 DoD Assessment Requirements.

    (b) 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/asda/dpc/cp/cyber/safeguarding.html#nistSP800171.
  - DFARS Clause 252.204-7020, NIST SP 800-171 DoD Assessment Requirements.

    (c) Requirements. 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 …, if necessary.

The Facts: DFARS Clauses Cont.

- Clauses requiring Sub-Contractor reporting of NIST SP 800-171 implementation
  - DFARS Clause 252.204-7020, NIST SP 800-171 DoD Assessment Requirements.

(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 items (excluding COTS 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.

The Facts: DFARS Clauses Cont.

- The Rescinded CMMC Clause
  - DFARS Clause 252.204-7021 Cybersecurity Maturity Model Certification Requirement.

a) Scope. The Cybersecurity Maturity Model Certification (CMMC) CMMC is a framework that measures a contractor's cybersecurity maturity to include the implementation of cybersecurity practices and institutionalization of processes (see https://www.acq.osd.mil/cmmc/index.html).

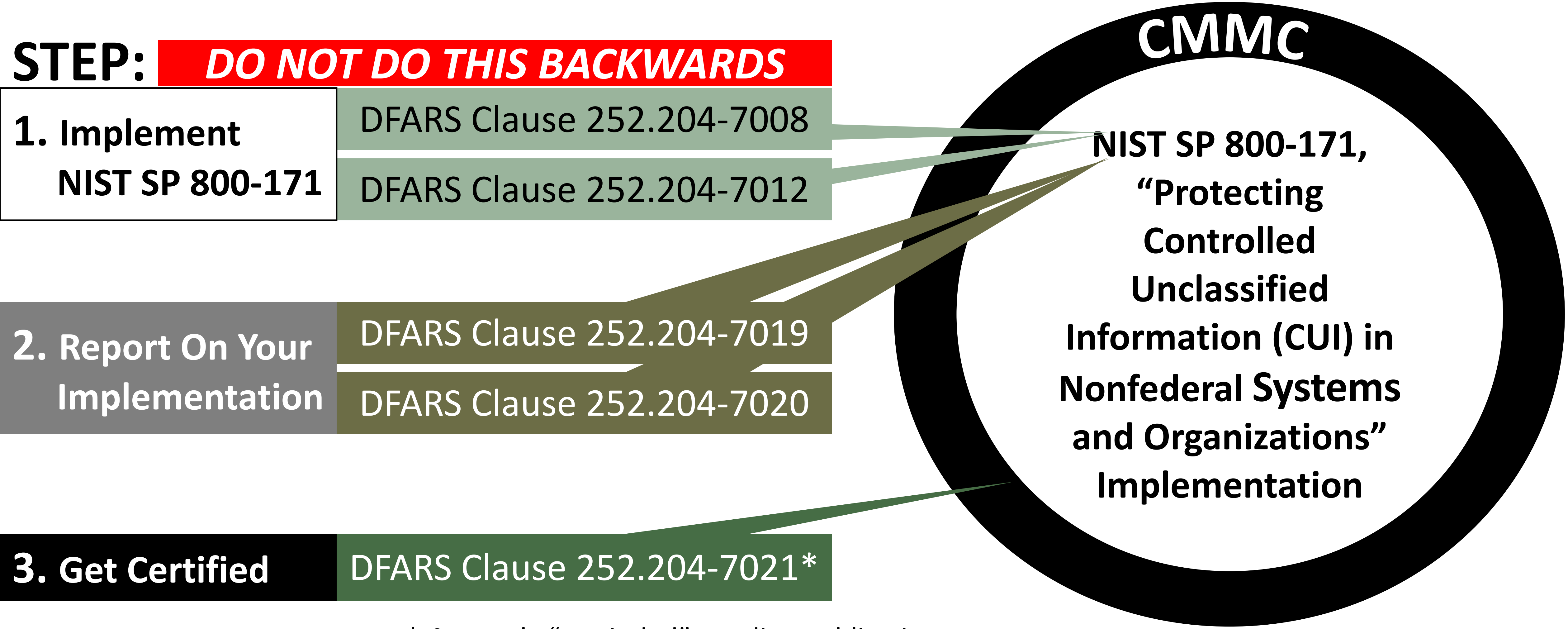
b) Requirements. The Contractor shall have a current (i.e. not older than 3 years) CMMC certificate at the CMMC level required by this contract and maintain the CMMC certificate at the required level for the duration of the contract.

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.

Myth Debunked



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

1. Implement NIST SP 800-171
   - DFARS Clause 252.204-7008
   - DFARS Clause 252.204-7012

2. Report On Your Implementation
   - DFARS Clause 252.204-7019
   - DFARS Clause 252.204-7020

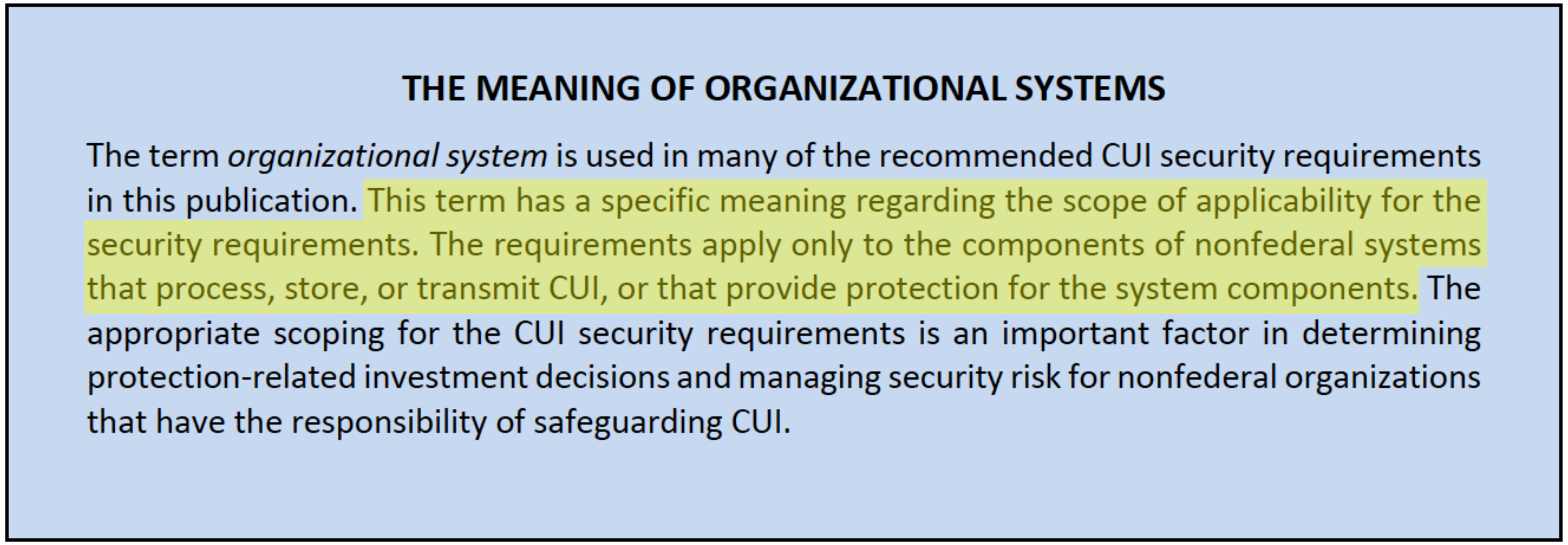
3. Get Certified
   - DFARS Clause 252.204-7021*

CMMC

NIST SP 800-171, "Protecting Controlled Unclassified Information (CUI) in Nonfederal Systems and Organizations" Implementation

* Currently "rescinded" pending publication

NIST SP 800-171 Scope of Applicability



THE MEANING OF ORGANIZATIONAL SYSTEMS

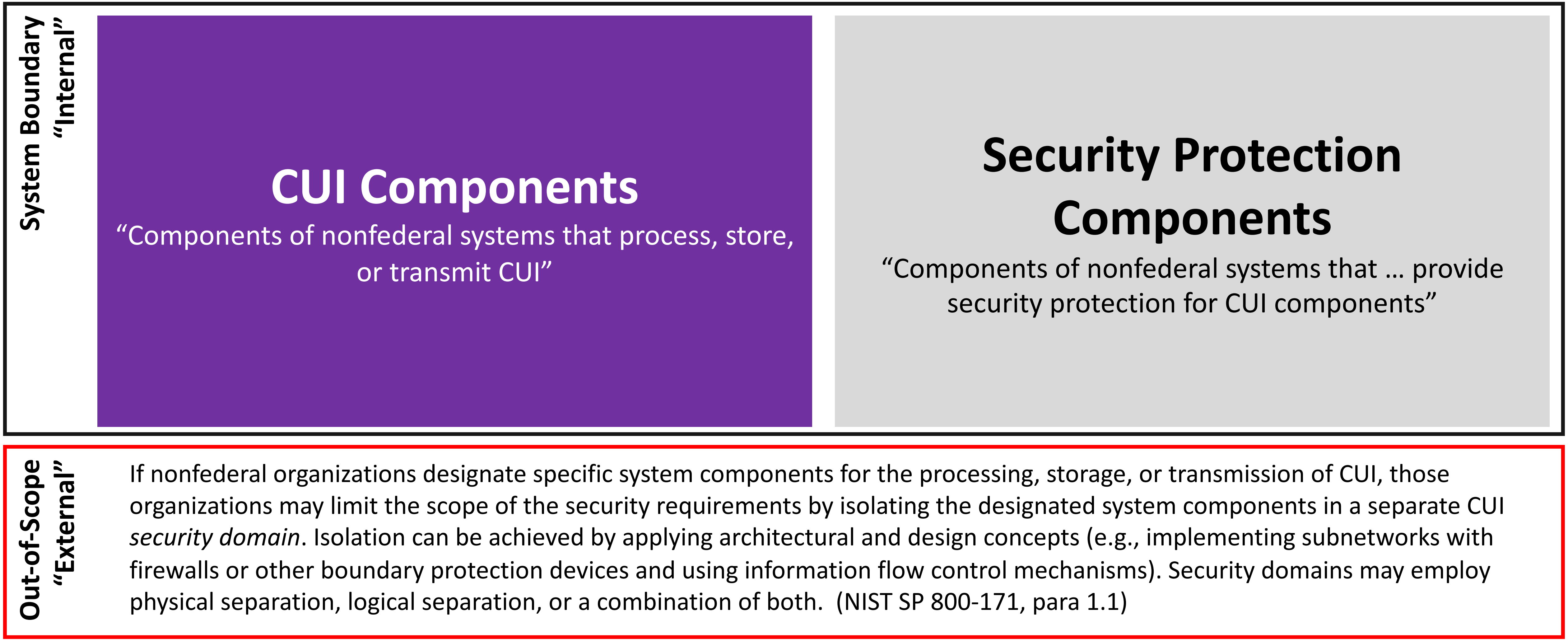
The term *organizational system* is used in many of the recommended CUI security requirements in this publication. This term has a specific meaning regarding the scope of applicability for the security requirements. The requirements apply only to the components of nonfederal systems that process, store, or transmit CUI, or that provide protection for the system components. The appropriate scoping for the CUI security requirements is an important factor in determining protection-related investment decisions and managing security risk for nonfederal organizations that have the responsibility of safeguarding CUI.

"The Scope of Applicability for the Security Requirements are the components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components."

- Para 1.1: "The requirements apply to components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components. 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*. …"

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”

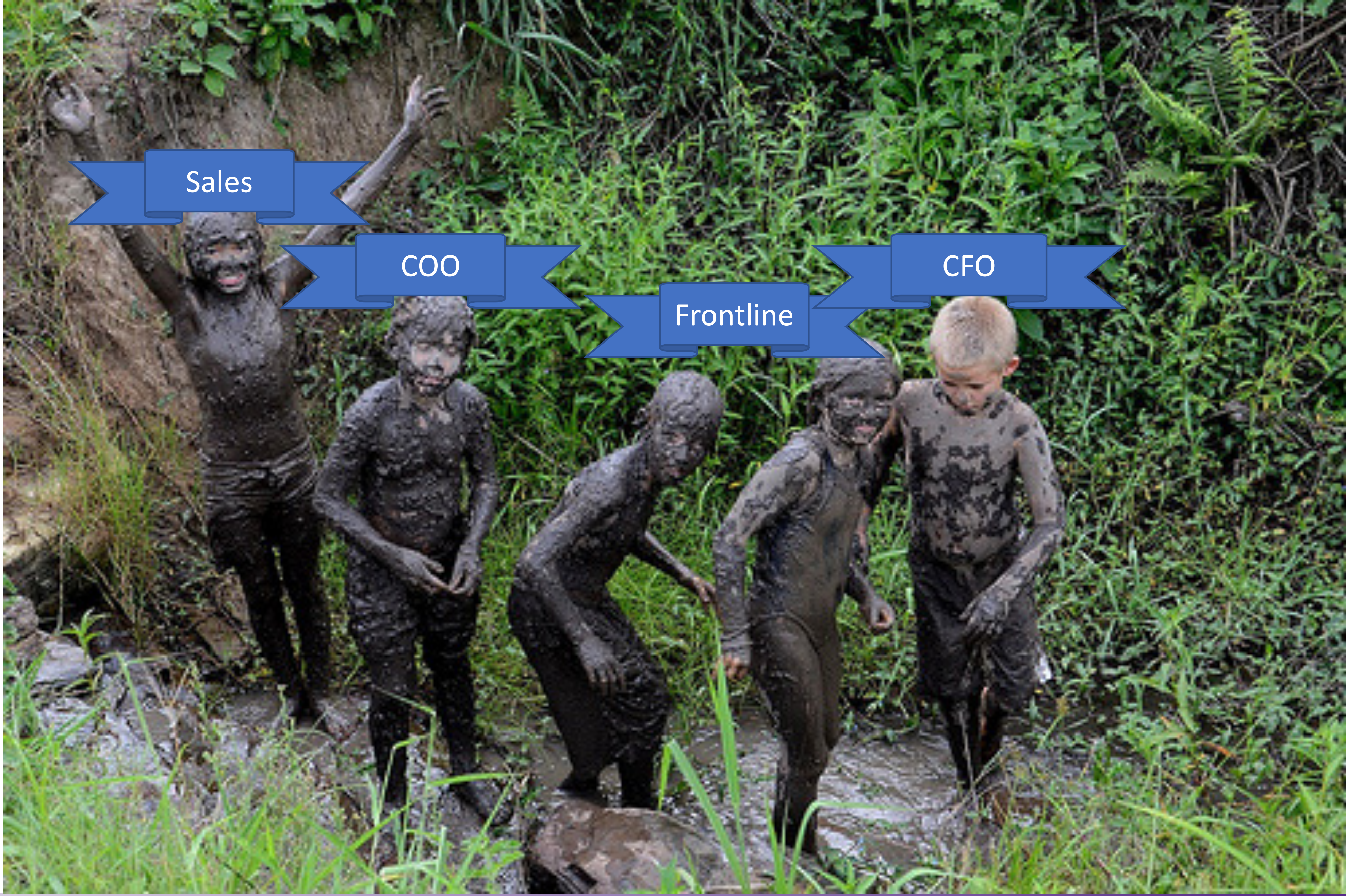
Security Protection Components

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

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)

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

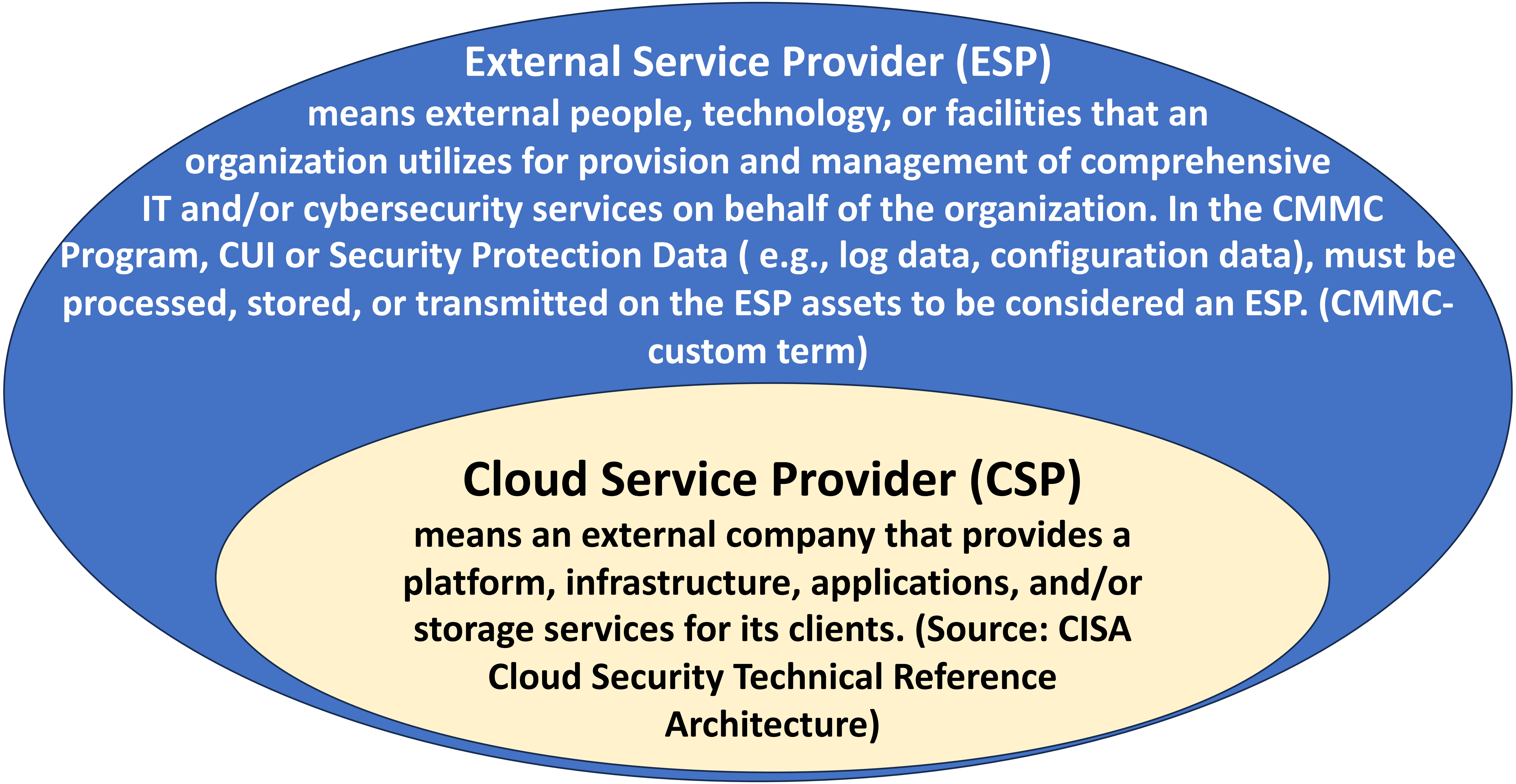


Steps to Apply the Scope of Applicability

1. Identify all contracts with DFARS -7008, -7012, or -7020 in them
2. Identify all processes involved with the contract(s) from bidding to closeout
3. Identify all people and facilities used in those processes
4. Identify all IT systems used by those people and facilities
5. Amongst the used IT System components, identify all the ones that process, store, or transmit CUI or “looks like CUI”
6. Identify the Security Protection components that protect the CUI-related IT system components
7. Identify all other Security protection components
8. Document all processes, people, facilities, and technologies in your scope diagram

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.**



External Service Provider (ESP)

means external people, technology, or facilities that an organization utilizes for provision and management of comprehensive IT and/or cybersecurity services on behalf of the organization. In the CMMC Program, CUI or Security Protection Data (e.g., log data, configuration data), must be processed, stored, or transmitted on the ESP assets to be considered an ESP. (CMMC-custom term)

Cloud Service Provider (CSP)

means an external company that provides a platform, infrastructure, applications, and/or storage services for its clients. (Source: CISA Cloud Security Technical Reference Architecture)

How to handle "The requirements apply to components…"

Lots of Drama in the ecosystem. Ignore it.

1. **Identify non-applicable requirements (e.g., wireless protection when you have no wireless) and document in your SSP's Not-Applicable Table**
2. **At the Assessment Objective (AO) to in-scope component level, apply the objectives**
3. **If the application of the AO requirement to Component is:**
    a) Successful, document it in the SSP and related documentation

    b) Simply not applicable (e.g., 3.13.2 Software Dev AOs), document the AO as "n/a" and add to your SSP N/A table as a partial

    c) For CUI (e.g., encrypt CUI) and this is a Security Protection Component, document the AO to Security Protection Component as "n/a" and explain in your SSP

    d) Unsuccessful and this is required, pursue "fixing" the component or document a compensating control (e.g., CNC computer can't have AV)

Steps to Apply the Scope of Applicability

1. Identify all contracts with DFARS -7008 or -7012 in them
2. Identify all processes involved with the contract(s) from bidding to closeout
3. Identify all people and facilities used in those processes
4. Identify all IT systems used by those people and facilities
5. Amongst the used IT System components, identify all the ones that process, store, or transmit CUI or "looks like CUI"
6. Identify the Security Protection components that protect the CUI-related IT system components
7. Identify all other Security protection components
8. Document all processes, people, facilities, and technologies in your scope diagram

The Real Enclaving Question…

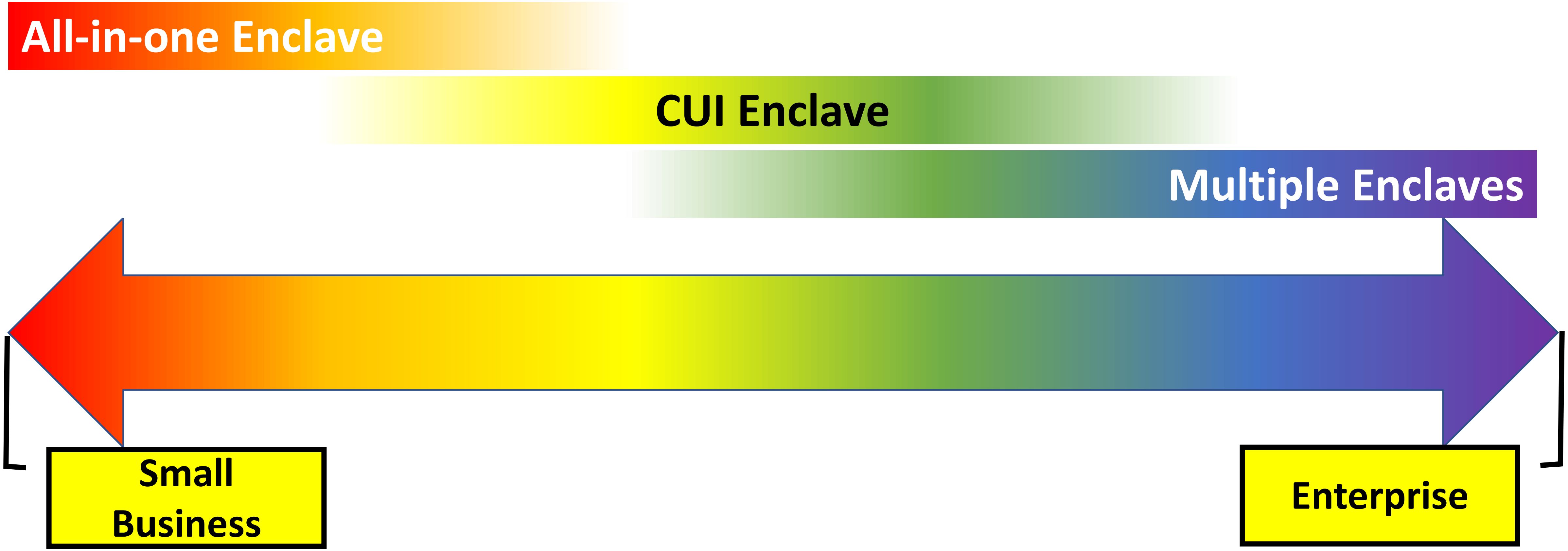
Given our processes that handle FCI/CUI, can we separate our processes to work on two-tiers of systems and still operate effectively?

- Why?
  - For most SMBs, enclaving is process driven.
  - The smaller your business is, the more everyone is involved in everything
  - The more everyone is involved in everything, then more than likely all supporting systems are involved too

Enclave Warning

Do NOT enclave by starting at the technical layer first

The Enclaving Spectrum



All-in-one Enclave

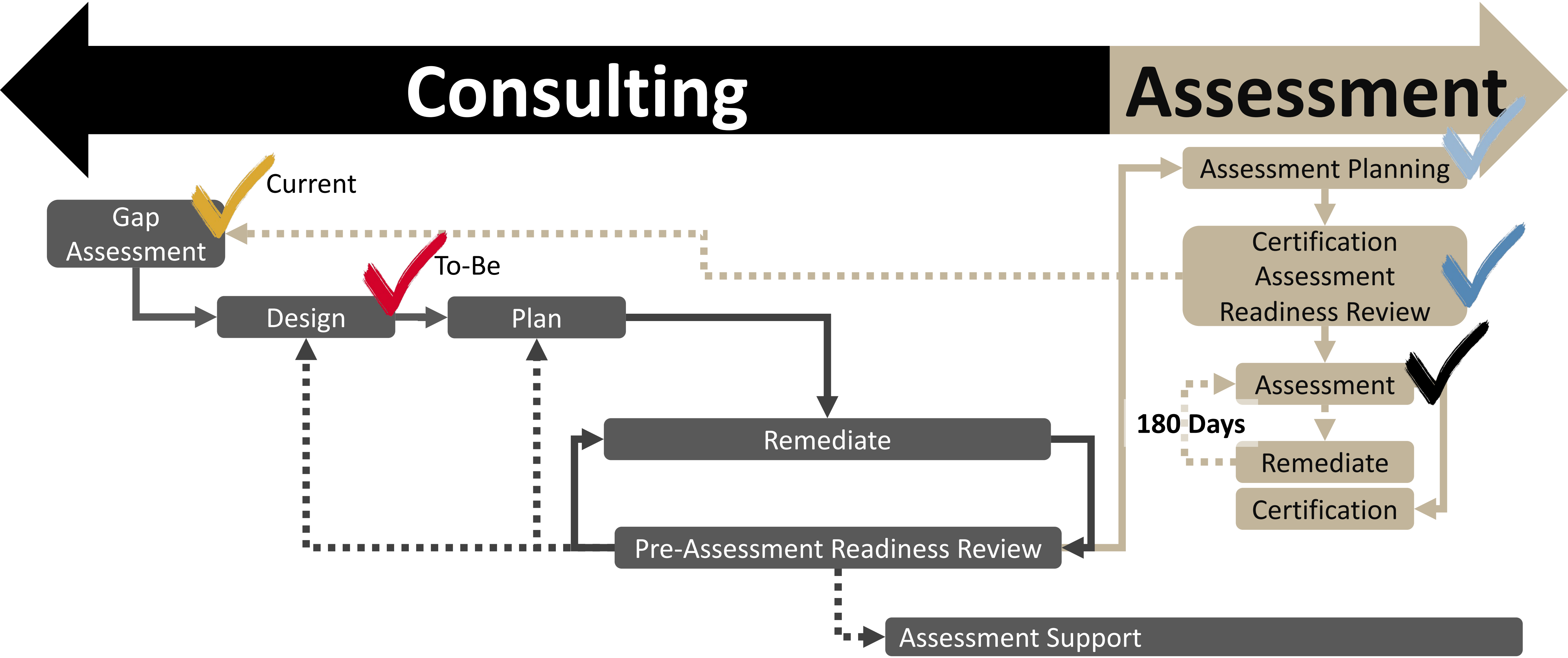
CUI Enclave

Multiple Enclaves

Small Business

Enterprise

Bonus: When to Apply the Scope of Applicability?



Consulting

Assessment

Current

Gap Assessment

To-Be

Design

Plan

Remediate

Pre-Assessment Readiness Review

Assessment Support

Assessment Planning

Certification Assessment Readiness Review

Assessment

180 Days

Remediate

Certification

CMMC Assessment Scope Guide

Identifying the CMMC Assessment Scope

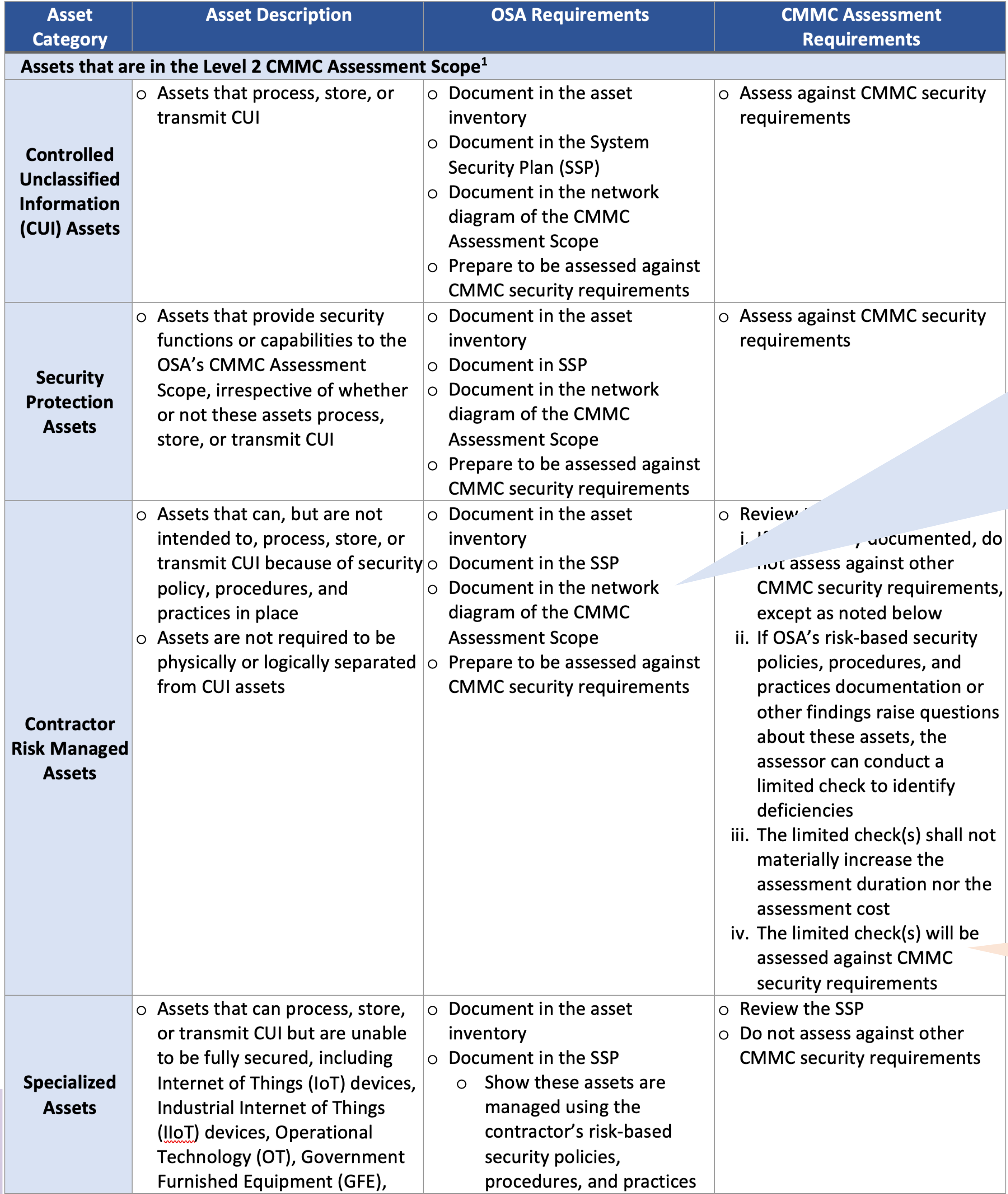
“An Assessment, as defined in 32 CFR § 170.4, means the testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization.

This document should help the reader understand the categorization of assets that, in turn, inform the specification of the boundary for a CMMC assessment. The scope of the CMMC Program does not include classified assets, even if they contain applicable Controlled Unclassified Information (CUI).

Prior to conducting a CMMC assessment, the OSA must specify the CMMC Assessment Scope as defined in 32 CFR § 170.19. The CMMC Assessment Scope defines which assets within the OSA’s environment will be assessed and the details of the assessment.

CMMC Assessment Scope, Level 2, Version 2.11,
As of December 2021, pg 2

CMMC Asset Categories Overview for Level 2



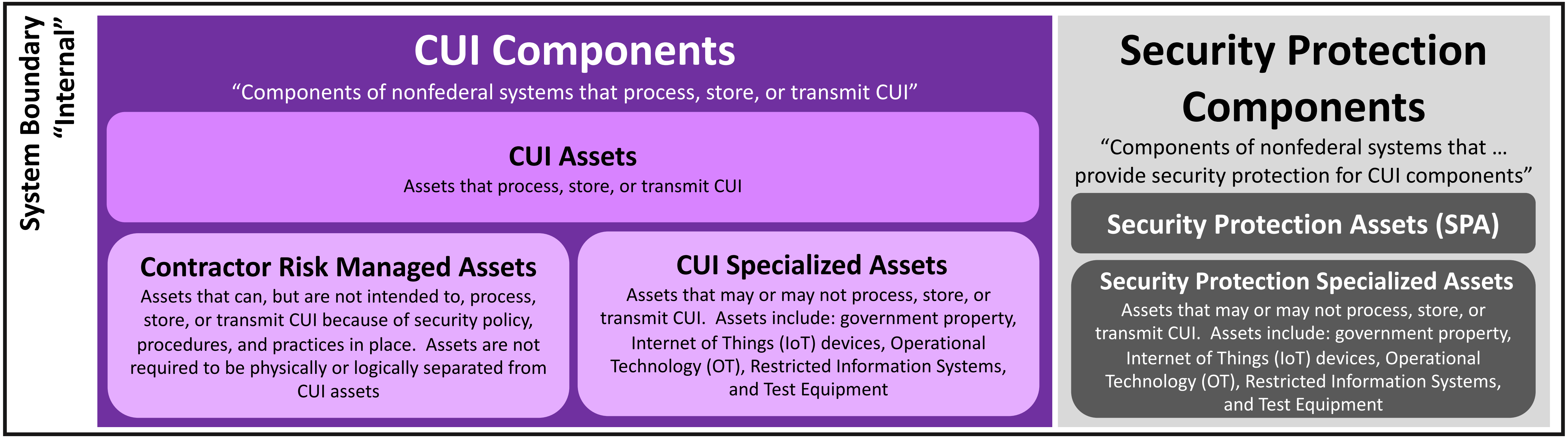
Asset Category	Asset Description	OSA Requirements	CMMC Assessment Requirements
Assets that are in the Level 2 CMMC Assessment Scope[1]			
Controlled Unclassified Information (CUI) Assets	○ Assets that process, store, or transmit CUI	○ Document in the asset inventory ○ Document in the System Security Plan (SSP) ○ Document in the network diagram of the CMMC Assessment Scope ○ Prepare to be assessed against CMMC security requirements	○ Assess against CMMC security requirements
Security Protection Assets	○ Assets that provide security functions or capabilities to the OSA's CMMC Assessment Scope, irrespective of whether or not these assets process, store, or transmit CUI	○ Document in the asset inventory ○ Document in SSP ○ Document in the network diagram of the CMMC Assessment Scope ○ Prepare to be assessed against CMMC security requirements	○ Assess against CMMC security requirements
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	○ Document in the asset inventory ○ Document in the SSP ○ Document in the network diagram of the CMMC Assessment Scope ○ Prepare to be assessed against CMMC security requirements	○ Review i. documented, do not assess against other CMMC security requirements, except as noted below ii. If OSA's risk-based security policies, procedures, and practices documentation or other findings raise questions about these assets, the assessor can conduct a limited check to identify deficiencies iii. The limited check(s) shall not materially increase the assessment duration nor the assessment cost iv. The limited check(s) will be assessed against CMMC security requirements
Specialized Assets	○ Assets that can process, store, or transmit CUI but are unable to be fully secured, including Internet of Things (IoT) devices, Industrial Internet of Things (IIoT) devices, Operational Technology (OT), Government Furnished Equipment (GFE),	○ Document in the asset inventory ○ Document in the SSP ○ Show these assets are managed using the contractor's risk-based security policies, procedures, and practices	○ Review the SSP ○ Do not assess against other CMMC security requirements

OSC must fundamentally document how "these assets are managed using the contractor's risk-based security policies, procedures, and practices"

C3PAO Conformity Assessment Restrictions

CUI-CON

NIST SP 800-171 Scope of Applicability <u>AND</u> CMMC Level 2 Assessment Scope



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

CUI 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”

Security Protection Assets (SPA)

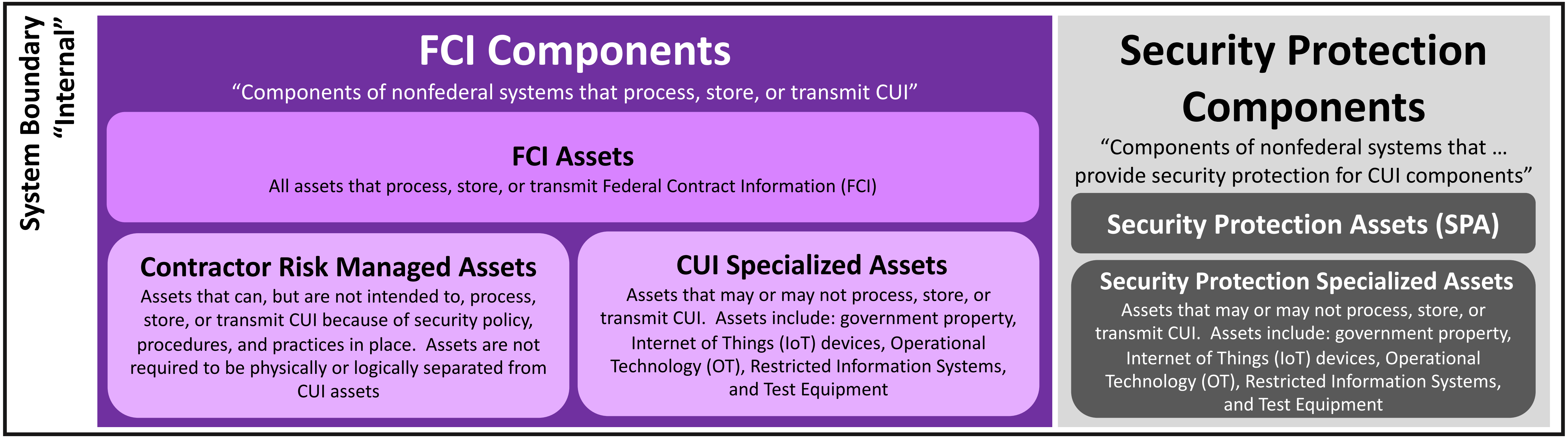
Security Protection Specialized Assets

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

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

CMMC Level 1 Assessment Scope



System Boundary
"Internal"

FCI Components

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

FCI Assets

All assets that process, store, or transmit Federal Contract Information (FCI)

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

CUI 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"

Security Protection Assets (SPA)

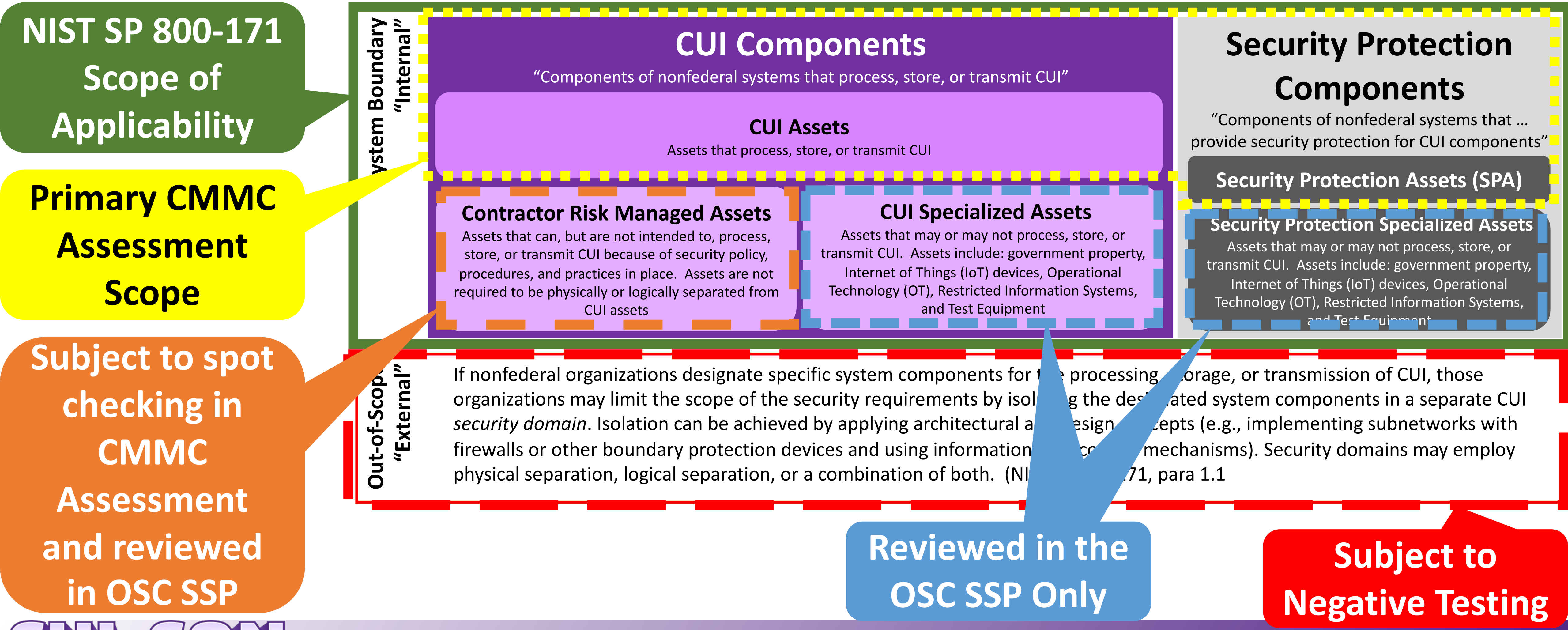
Security Protection Specialized Assets

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

Out-of-Scope
"External"

If nonfederal organizations designate specific system components for the processing, storage, or transmission of FCI, 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

NIST SP 800-171 Scope of Applicability AND CMMC Level 2 Assessment Scope



NIST SP 800-171 Scope of Applicability

Primary CMMC Assessment Scope

Subject to spot checking in CMMC Assessment and reviewed in OSC SSP

ystem 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

CUI 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”

Security Protection Assets (SPA)

Security Protection 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

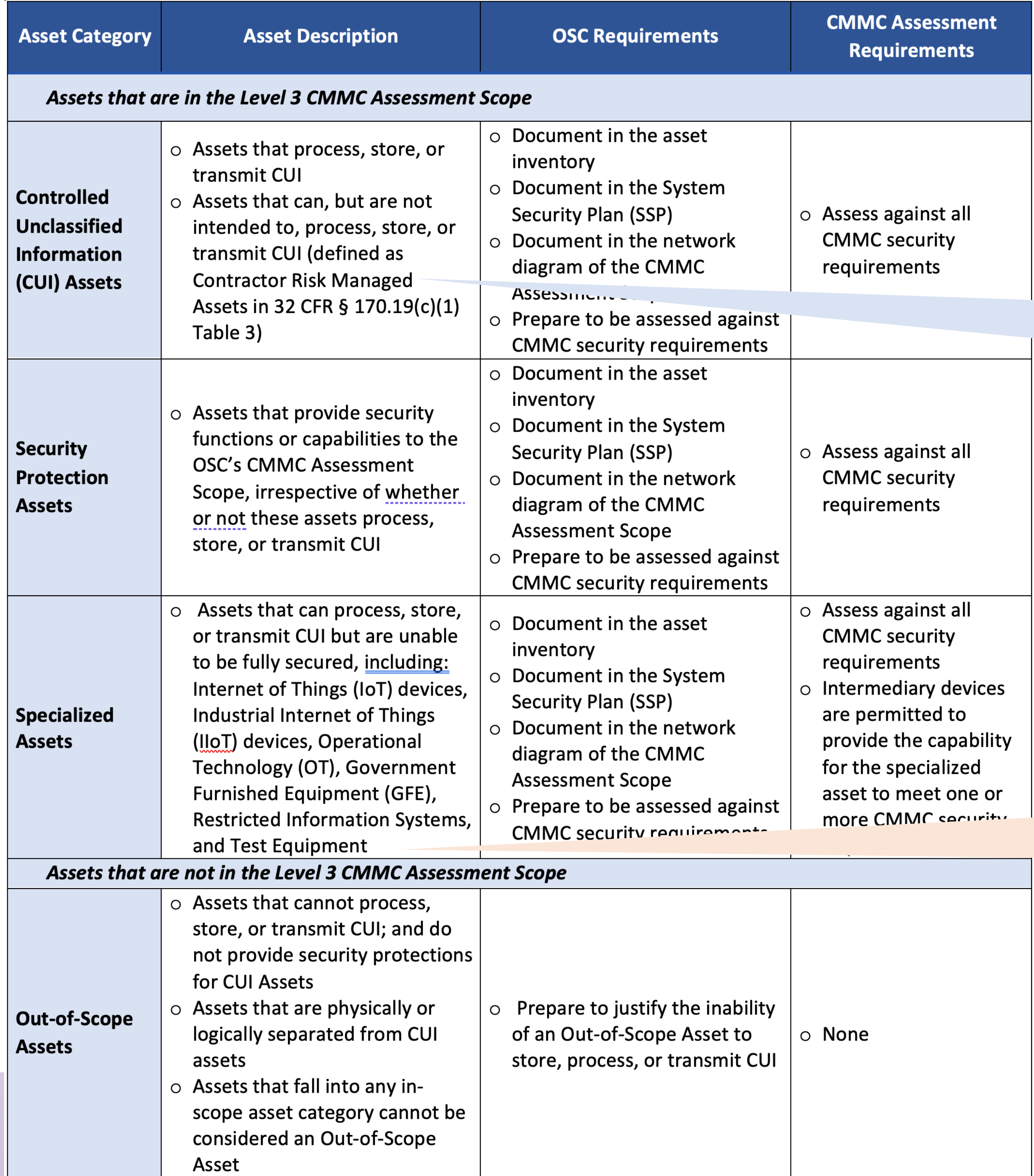
Out-of-Scop “External”

If nonfederal organizations designate specific system components for t e processing, orage, or transmission of CUI, those organizations may limit the scope of the security requirements by isol g the des ated system components in a separate CUI *security domain*. Isolation can be achieved by applying architectural a esign cepts (e.g., implementing subnetworks with firewalls or other boundary protection devices and using information co mechanisms). Security domains may employ physical separation, logical separation, or a combination of both. (NI 71, para 1.1

Reviewed in the OSC SSP Only

Subject to Negative Testing

CMMC Asset Categories Overview for Level 3



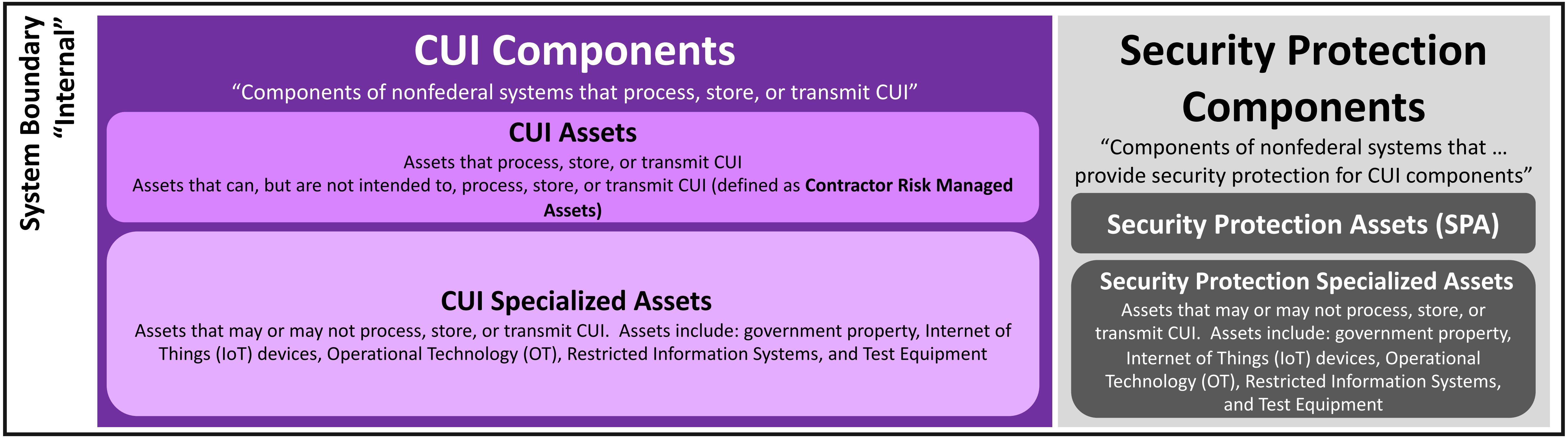
Asset Category	Asset Description	OSC Requirements	CMMC Assessment Requirements
Assets that are in the Level 3 CMMC Assessment Scope			
Controlled Unclassified Information (CUI) Assets	○ Assets that process, store, or transmit CUI ○ Assets that can, but are not intended to, process, store, or transmit CUI (defined as Contractor Risk Managed Assets in 32 CFR § 170.19(c)(1) Table 3)	○ Document in the asset inventory ○ Document in the System Security Plan (SSP) ○ Document in the network diagram of the CMMC Assessment Scope ○ Prepare to be assessed against CMMC security requirements	○ Assess against all CMMC security requirements
Security Protection Assets	○ Assets that provide security functions or capabilities to the OSC's CMMC Assessment Scope, irrespective of whether or not these assets process, store, or transmit CUI	○ Document in the asset inventory ○ Document in the System Security Plan (SSP) ○ Document in the network diagram of the CMMC Assessment Scope ○ Prepare to be assessed against CMMC security requirements	○ Assess against all CMMC security requirements
Specialized Assets	○ Assets that can process, store, or transmit CUI but are unable to be fully secured, including: Internet of Things (IoT) devices, Industrial Internet of Things (IIoT) devices, Operational Technology (OT), Government Furnished Equipment (GFE), Restricted Information Systems, and Test Equipment	○ Document in the asset inventory ○ Document in the System Security Plan (SSP) ○ Document in the network diagram of the CMMC Assessment Scope ○ Prepare to be assessed against CMMC security requirements	○ Assess against all CMMC security requirements ○ Intermediary devices are permitted to provide the capability for the specialized asset to meet one or more CMMC security
Assets that are not in the Level 3 CMMC Assessment Scope			
Out-of-Scope Assets	○ Assets that cannot process, store, or transmit CUI; and do not provide security protections for CUI Assets ○ Assets that are physically or logically separated from CUI assets ○ Assets that fall into any in-scope asset category cannot be considered an Out-of-Scope Asset	○ Prepare to justify the inability of an Out-of-Scope Asset to store, process, or transmit CUI	○ None

CRMAs now fully in scope

Specialized Assets now fully in scope

CUI-CON

NIST SP 800-171 Scope of Applicability AND CMMC Level 3 Assessment Scope



System Boundary
"Internal"

CUI Components

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

CUI Assets

Assets that process, store, or transmit CUI
Assets that can, but are not intended to, process, store, or transmit CUI (defined as **Contractor Risk Managed Assets)**

CUI 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"

Security Protection Assets (SPA)

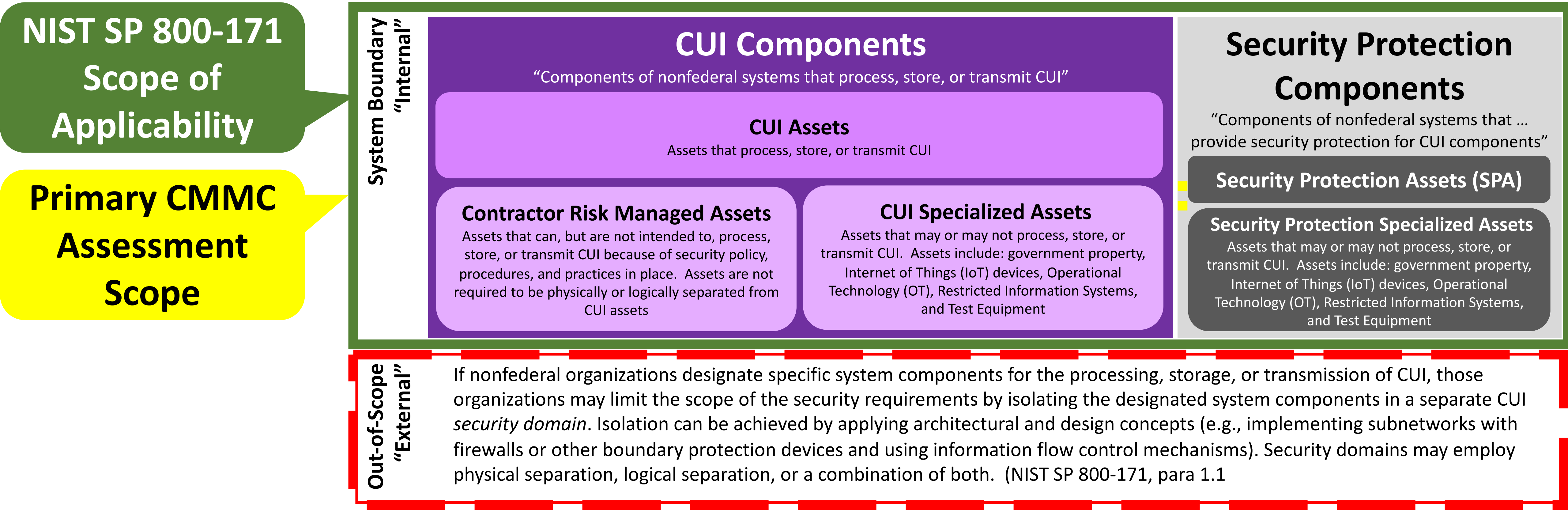
Security Protection Specialized Assets

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

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

NIST SP 800-171 Scope of Applicability AND CMMC Level 3 Assessment Scope



NIST SP 800-171 Scope of Applicability

Primary CMMC Assessment Scope

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

CUI 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"

Security Protection Assets (SPA)

Security Protection 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

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

CMMC Level 3 Enclave???

- §170.19(e):
  - “Relationship between Level 2 and Level 3 CMMC Assessment Scope. The Level 3 CMMC Assessment Scope must be equal to or a subset of the Level 2 CMMC Assessment Scope in accordance with § 170.18(a), e.g., a Level 3 data enclave with greater restrictions and protections within a Level 2 data enclave. Any Level 2 POA&M items must be closed prior to the initiation of the CMMC Level 3 Certification Assessment. DCMA DIBCAC may check any Level 2 security requirement of any in-scope asset, and if they determine a requirement is NOT MET, DCMA DIBCAC may allow for remediation or may immediately terminate the Level 3 Assessment.”

The Real Enclaving Question…

Given our processes that handle “Level 3 CUI,” can we separate our processes to work on two-tiers of systems and still operate effectively?

- Why?
  - For most SMBs, enclaving is process driven.
  - The smaller your business is, the more everyone is involved in everything
  - The more everyone is involved in everything, then more than likely all supporting systems are involved too

As the CMMC Churns

THE CYBER AB
CMMC CERTIFICATION
AUTHORIZED C3PAO

CAICO
CERTIFIED CMMC ASSESSOR

CAICO
CERTIFIED CMMC PROFESSIONAL

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