CYBERSECURITY MATURITY MODEL CERTIFICATION

HOW GOVERNMENT CONTRACTORS CAN PREPARE

March 15, 2023

Agenda

1	What Is Federal Contract Information (FCI) and How to Identify It
2	What Is DFARS 252.204-7012 and What Is CMMC?
3	What Is Controlled Unclassified Information (CUI) and How to Identify It
4	DoD Instruction 5200.48
5	When to Expect CMMC 2.0 Rulemaking to Be Finalized and When You Might See It in Your Contracts
6	Tips and Strategies for CMMC Compliance and What You Need to Know
7	Tips for Passing an Assessment

WITH YOU TODAY

CHRISTINA REYNOLDS
Industry Specialty Services Director

STACY HIGH-BRINKLEY
Industry Specialty Services Sr Manager

What Is FCI?

FAR Clause: FAR 52.204-21

UNDERSTANDING “BASIC CYBER HYGIENE”

FAR 52.204-21
Basic Safeguarding of Covered Contractor Information Systems

Defines FCI

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.

Safeguarding

Requires application of basic safeguarding requirements when processing, storing, or transmitting Federal Contract Information (FCI) in or from covered contractor information systems.

Defines **“Basic Cyber Hygiene”**

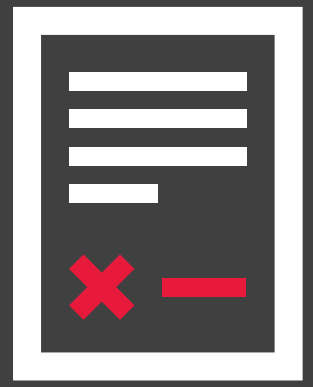
17 Security Controls to Implement

Mandatory Flow-down to Subcontractors

Examples of FCI Documents

SPECIFIC EXAMPLES OF FCI INCLUDE

- Contract information
- Emails exchanged with the DoD or defense contractor
- Proposal responses
- Contract performance reports
- Organizational or programmatic charts
- Process documentation
- Past performance information



Because every DoD contract contains FCI, every contractor will require at least CMMC Level 1

CUI//SP-PROPIN

When FCI is marked as CUI

- **Business Proprietary information** (CUI//SP-PROPIN)
- *Material and information relating to, or associated with, a company's products, business, or activities, including but not limited to financial information; data or statements; trade secrets; product research and development; existing and future product designs and performance specifications.*
  - Used by Govt to secure FCI information:
    - Proposal cost data / rate structure
    - Approved accounting system documentation

What NARA says PROPIN is:

Is my Proprietary Information CUI?

NARA Answer: The government will protect it as CUI (and may even send it back to you as CUI) but the proprietary information you create internally and maintain ownership of is not CUI (though it may require protections pursuant to other laws or regs).

(Stakeholder Q2 Agenda slides)

Federal Register vol 81 No 178 Sept 14, 2016

(h) *Controlled Unclassified Information* (CUI) is information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.

However, CUI does not include classified information (see paragraph (e) of this section) or information a nonexecutive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency.

FCI & CUI Venn Diagram

FCI Applies to

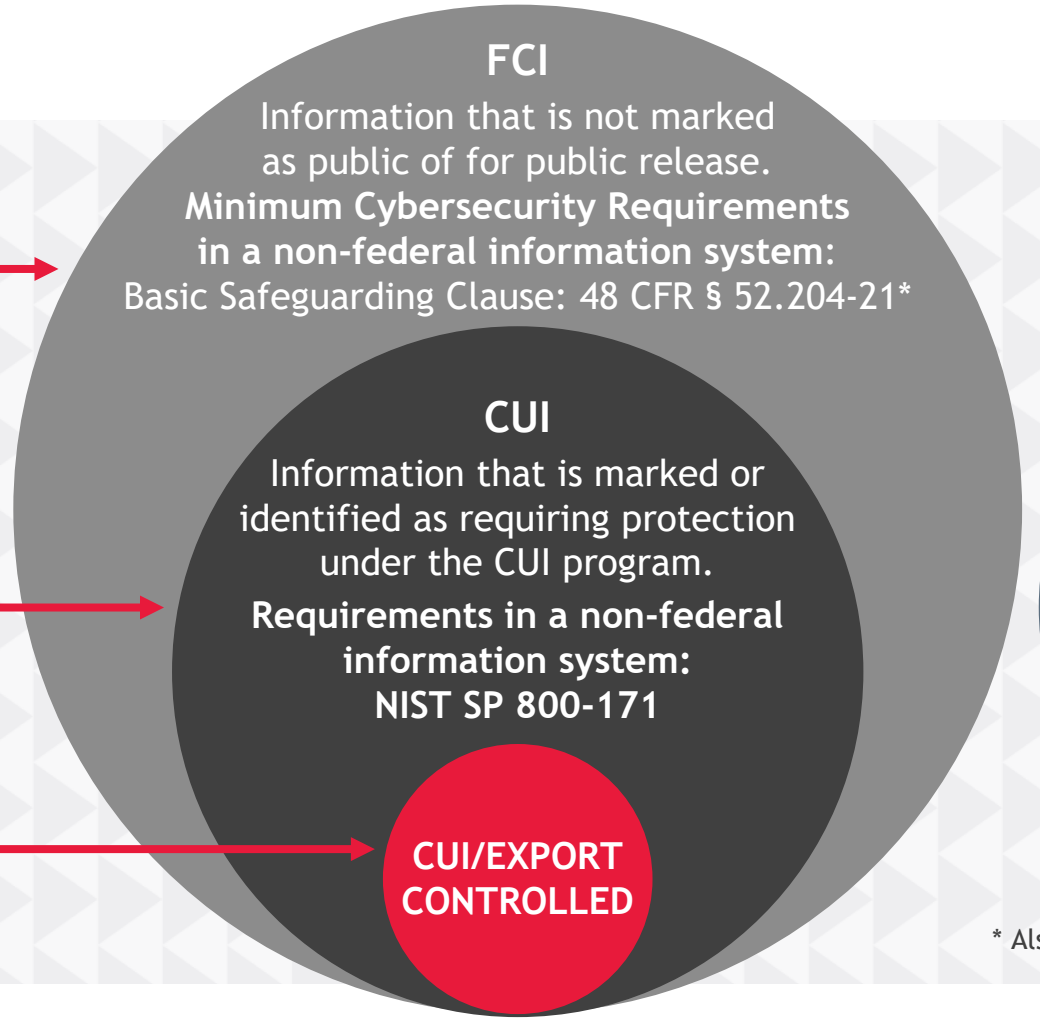
- Minimum Baseline for all DIB Contractors
- Contract Award/Mod/Action
- Sent to Contractor directly
- Non-publicly posted data

CUI Applies to

- Data Marked by Govt as CUI
- Data generated by contractor that requires CUI markings

CUI/Export Controlled Applies to

- Export-Controlled Data that may require U.S. Data Sovereignty



Public contract information posted in BetaSAM.gov

Public Information

Public information or information marked for public release. **Requirements in a non-federal information system:** None

Cannot contain FCI or CUI

* Also excludes simple transactional information.

What Is CUI?

DFARS 252.204-7012

SAFEGUARDING FOR CONTROLLED UNCLASSIFIED INFORMATION (CUI)

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

Defines CUI

Law, regulation or Government-wide policy requires to have safeguarding or disseminating controls, excluding information that is classified under EO 13526.

NARA archives: Classification for CUI Categories
https://www.archives.gov/cui/registry/category-list

Exemption: Manufacturers of COTS / Commercial Items

Provide "Adequate Security"
NIST SP 800-171

→ **System Security Plan (SSP)**
requirements **to be implemented**

→ **Plan of Action and Milestones (POA&M)**
requirements **not yet implemented**

Mandatory Flow down Clause to Subcontractors

Safeguard Covered Defense Information (CDI)
(read: CUI)

Report Cyber Incidents within 72 hours: DIBNET
DoD Cyber Crime Center (DC3).

Report Malicious SW
Facilitate Damage Assessment

What Is CUI?

Controlled Unclassified Information
(32 CFR 2002.4)

- **Information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government**, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls

***CUI does not include** classified information

CUI Basic, CUI Specified, or Both?

Law, regulation, or government-wide policy may require or permit safeguarding or dissemination controls in three ways:

CUI BASIC

Types of CUI that have a general requirement for safeguarding or disseminating controls and sets a uniform set of handling requirements for all agencies to use on all types of CUI Basic.

All CUI Basic categories will be controlled by the same standard—no less than 'moderate' confidentiality, the lowest possible control level above the 'low' standard already applied to all information systems without CUI.

CUI Basic requirements are the baseline default requirements for protecting CUI and apply to the vast majority to CUI.

CUI SPECIFIED

CUI Specified recognizes the types of CUI that have required or permitted controls included in their governing authorities, and each CUI Specified category or subcategory applies those other controls as required or permitted by the governing law, regulation, or policy.

CUI Specified information may be handled at higher confidentiality levels if the authorities establishing and governing the CUI Specified category or subcategory allow or require a higher confidentiality level or more specific or stringent controls. If they do not, then the no-less-than moderate confidentiality level applies

CUI SPECIFIED
but with CUI Basic controls

Where the authority does not specify: Requiring or permitting agencies to control the information and specifying only some of those controls, which makes the information CUI Specified, but with CUI Basic controls where the authority does not specify.

How to Reference Basic/Specified CUI Controls

BASIC

SPECIFIED

CUI Categories

- CUI Categories are listed alphabetically within organizational index grouping.
- Select a Category to view associated detail information.

Organizational Index Grouping	CUI Categories
Critical Infrastructure	• Ammonium Nitrate • Chemical-terrorism Vulnerability Information • Critical Energy Infrastructure Information • Emergency Management • General Critical Infrastructure Information • Information Systems Vulnerability Information • Physical Security • Protected Critical Infrastructure Information • SAFETY Act Information • Toxic Substances • Water Assessments
Defense	• Controlled Technical Information • DoD Critical Infrastructure Security Information • Naval Nuclear Propulsion Information • Unclassified Controlled Nuclear Information - Defense

Source: CUI Categories | National Archives

EXAMPLE: DEFENSE

Controlled Technical Information (CTI)

CUI Category: Controlled Technical Information

Banner Marking: CUI//SP-CTI

Category Description:	Controlled Technical Information 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. Controlled technical information is to be marked with one of the distribution statements B through F, in accordance with Department of Defense Instruction 5230.24, "Distribution Statements of Technical Documents." The term does not include information that is lawfully publicly available without restrictions. "Technical Information" means technical data or computer software, as those terms are defined in Defense Federal Acquisition Regulation Supplement clause 252.227-7013, "Rights in Technical Data - Noncommercial Items" (48 CFR 252.227-7013). 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.
Category Marking:	CTI
Banner Format and Marking Notes:	Banner Format: CUI//Category Marking//Limited Dissemination Control Marking Notes: • The CUI Control Marking may consist of either the word "CONTROLLED" or the acronym "CUI", depending on agency policy. • Category marking is optional when marking Basic CUI unless required by agency policy. Example: CUI//Limited Dissemination Control. • Category Marking preceded by "SP-" is required when marking Specified CUI. Example: CUI//SP-Category Marking//Limited Dissemination Control • Whether CUI is Basic or Specified is determined by the applicable Safeguarding and/or Dissemination Authority for a given instance of CUI. • Separate multiple Category Markings by a single forward slash (/) and list Category Markings alphabetically. Example: CUI//Category Marking A/Category Marking B//Limited Dissemination Control • Category Markings for Specified CUI precede Category Markings for Basic CUI. Example: CUI//SP-Category Marking/Category Marking//Limited Dissemination Control • Separate multiple Limited Dissemination Controls by a single forward slash (/). Example: CUI//Category Marking//Limited Dissemination Control/Limited Dissemination Control • Reference 32 CFR 2002.20 , CUI Marking Handbook , Limited Dissemination Controls and individual agency policy for additional and specific marking guidelines

Source: CUI Category: Controlled Technical Information | National Archives

Example – Defense: Controlled Technical Information (CTI)

BOTTOM OF PAGE

Notes for Safeguarding, Dissemination and Sanction Authorities:

- Whether CUI is Basic or Specified is determined by the applicable Safeguarding and/or Dissemination Authority for that CUI.
- Each "Safeguarding and/or Dissemination Authority" citation links to the statute, regulation or government-wide policy authorizing the control of that information as CUI.
- Each "Sanctions" authority links to the statute, regulation or government-wide policy that includes penalties for CUI misuse of CUI for the associated "Safeguarding and/or Dissemination Authority" on the same line.

Safeguarding and/or Dissemination Authority	Basic or Specified	Banner Marking	Sanctions
48 CFR 252.204-7012	Specified	CUI//SP-CTI	

Authority links are updated based on regular re-publication of the United States Code and Code of Federal Regulations, and the CUI Registry maintenance schedule.

Source: CUI Category: Controlled Technical Information | National Archives

Basic or Specified? The NARA CUI Categories

SPECIFIED

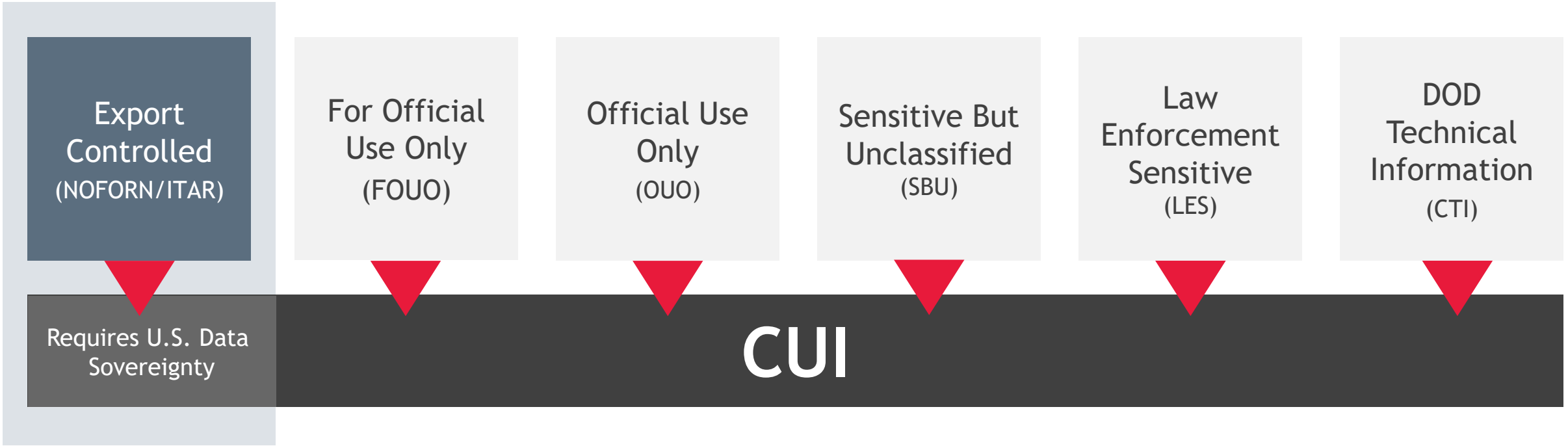
BASIC

CUI Category	Banner Marking: Specified Authorities	Banner Marking: Basic Authorities	Category Marking	Organizational Index Grouping
Accident Investigation	CUI//SP-AIV		AIV	Law Enforcement
Administrative Proceedings	CUI//SP-ADPO	CUI	ADPO	Legal
Agriculture		CUI	AG	Intelligence
Ammonium Nitrate	CUI//SP-CRITAN		CRITAN	Critical Infrastructure
Archaeological Resources	CUI//SP-ARCHR		ARCHR	Natural and Cultural Resources
Asylee		CUI	ASYL	Immigration
Bank Secrecy	CUI//SP-FSEC	CUI	FSEC	Financial
Battered Spouse or Child		CUI	BATT	Immigration
Budget	CUI//SP-BUDG		BUDG	Financial
Campaign Funds	CUI//SP-FUND		FUND	Law Enforcement
Chemical-terrorism Vulnerability Information	CUI//SP-CVI	CUI	CVI	Critical Infrastructure

Source: https://www.archives.gov/cui/registry/category-marking-list

What Is CUI?

HOW DO YOU KNOW IF CUI DATA IS ALREADY ON YOUR SYSTEMS?

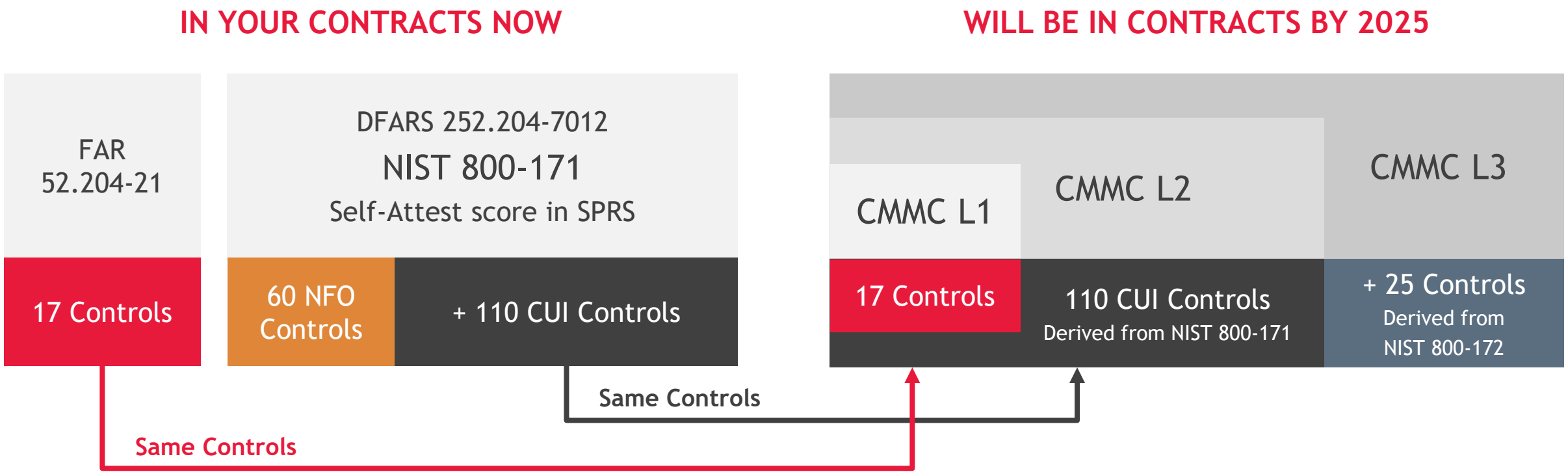


DoD Instruction 5200.48
Marking Guide: fas.org/sgp/cui/marking-2016.pdf

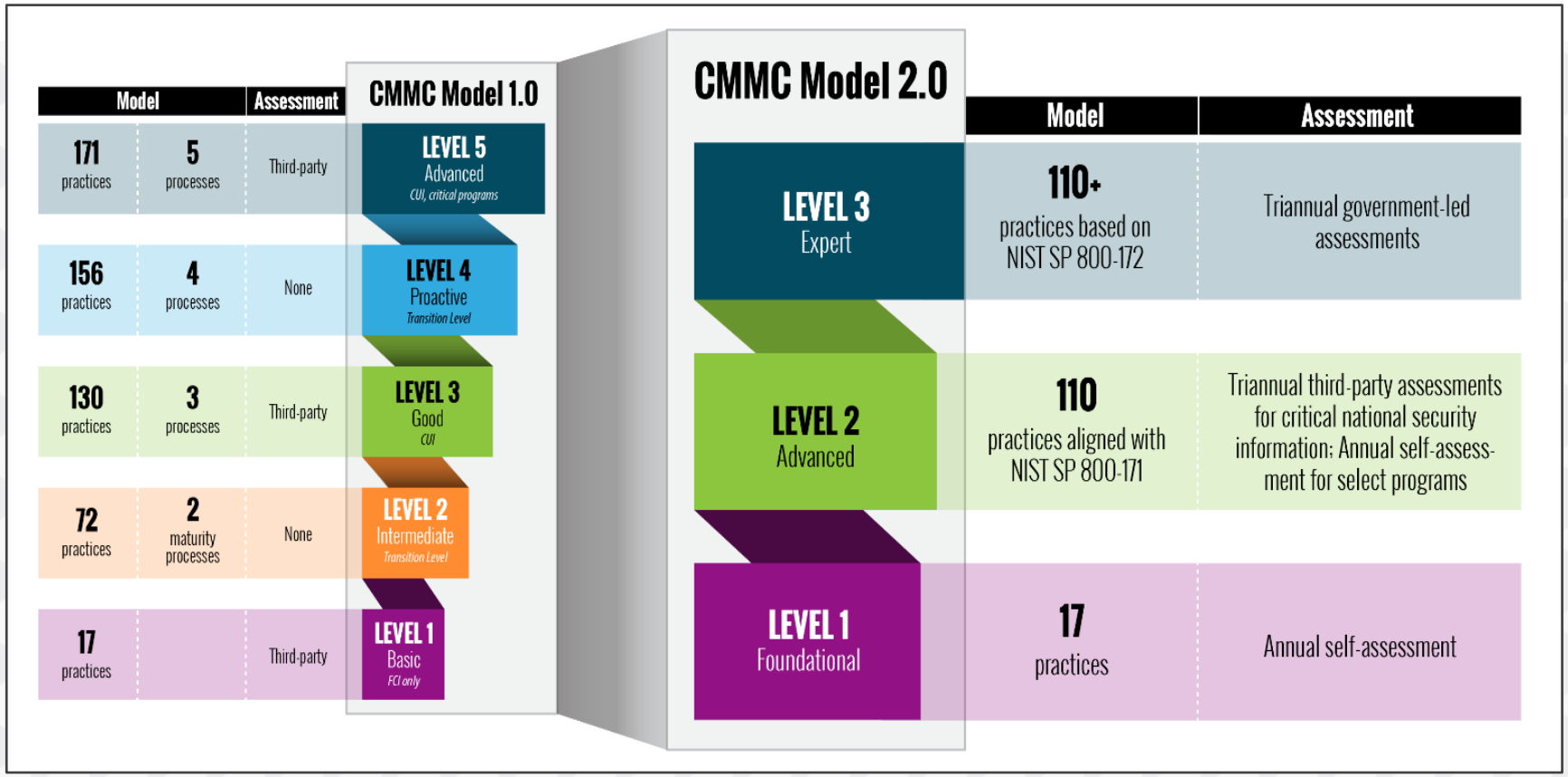
Know Your Contract Requirements

DFARS 7012 Vs CMMC

Security Controls and Inheritance Between Frameworks



CMMC 2.0 Processes



Source: CMMC Model (defense.gov)

The “Other” DFARS Clauses

DFARS 252.204-7019

Notice of NIST SP 800-171 DOD Assessment Requirements

- Amends DFARS 7012 by requiring KOs to verify offeror has current NIST 800-171 Assessment on record
- Summary-level assessment scores (out of 110) must be uploaded to SPRS
- Assessments may not be more than 3 years old, entered per CAGE code

DFARS 252.204-7020

NIST SP 800-171, DOD Assessment Requirements

- Provides DOD NIST SP 800-171 Assessment Methodology, formerly used during DIBCAC assessments, based on NIST 800-171 controls and a scoring range of -205 up to 110
- Basic, Medium, High-level assessments

DFARS 252.204-7021

Contractor Compliance with the Cybersecurity Maturity Model Certification (CMMC) Level Requirements

- Cybersecurity Maturity Model Certification Requirements
- Prescribed for use in solicitations and contracts, including FAR part 12 procedures for the acquisition of commercial items (ex. COTS)

Overview of CMMC 2.0 Assessments

CMMC Level 1
FAR 52.204-21 – 17 Controls

Self-Attest Yearly

Contractors who do not handle information Covered Defense Information (CDI) will be required to perform annual self-assessments against clearly articulated cybersecurity standards.

SPRS
Self-Attestation

CMMC Level 2
NIST 800-171 – 110 Controls

Self-Attest Yearly

Certify every 3 years

Contractors managing Covered Defense Information (CDI) will be required to undergo third-party assessments.

SPRS
C3PAO Certification

CMMC Level 3
NIST 800-171 (110 controls) + NIST 800-172 (26? controls – not final)

Self-Attest Yearly

Certify every 3 years

The highest priority, most critical defense programs will require government-led assessments.

SPRS
DIBCAC Assessment

NIST 800-171 Rev 3 Coming

- Things to expect (from NIST):
  - Improve alignment between the CUI Series and other frameworks
  - Updates for consistency with SP 800-53 Rev 5 and SP 800-53B (Moderate impact baseline)
  - Updates to improve usability and implementation

"Over the next 18 months we're going to be updating 800-171, 800-171A, and most likely 800-172 and 800-172A"

- Ron Ross | NIST Fellow 8/15/22

- Rumors/concerns from comments
  - Non-Federal Organization (NFO) controls will become more prominent
  - May see the delta-20 controls, especially recovery, come back from CMMC 1.0
  - Most commented issue was 3.13.11 – Employ FIPS validated cryptography when used to protect the confidentiality of CUI – Why the concern? One word – MSPs.
  - Addressing technology-specific implementations – e.g. Zero Trust architectures
  - May send CAP (CMMC Assessment Process for C3PAOs) back for revisions to add new controls tailored back into ***CUI baseline***

CMMC Rulemaking

Information You Should Know
Regarding the CMMC 2.0 Final Rule

Latest on CMMC Rule Making

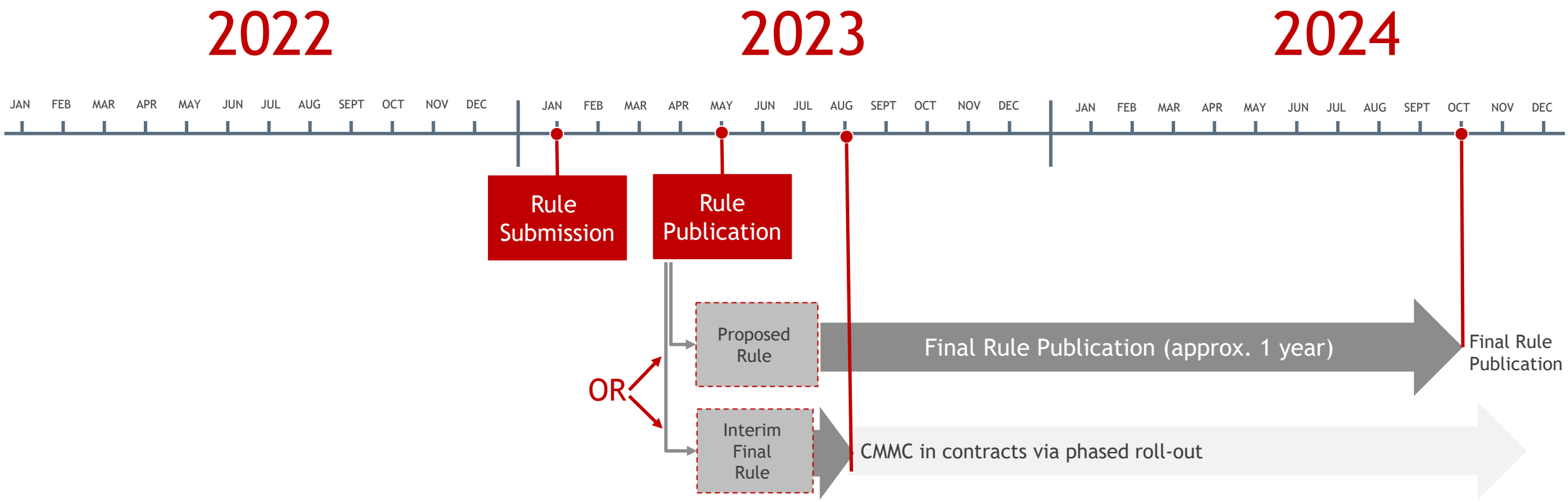
RULE MAKING

- The rulemaking process and timelines can take up to 24 months. CMMC 2.0 will become a contract requirement once rulemaking is completed
- Agenda Published: 4 January 2023
- Proposed Rule: May 2023
  - DASHBOARD - REGINFO.GOV

CMMC REQUIREMENTS WITHIN CONTRACTS

- What will be my obligations when the interim rule is issued?
- What are my obligations now versus when the CMMC final rule is applied?
- Will it hit existing contracts or just new contracts?

Timeline to CMMC Compliance is still 2025



[View Rule (reginfo.gov)]

CMMC Requirements

CMMC REQUIREMENTS WITHIN CONTRACTS

- **What are my obligations now versus when the CMMC final rule is applied?**
  - Self-Attest and upload SPRS scores yearly vs. Third Party Assessment
- **Will it hit existing contracts or just new contracts?**
  - CMMC will be a phased approach – starting with new contracts, including option years

The False Claims Act

WHY YOU NEED TO UNDERSTAND BEFORE POSTING A SCORE TO SPRS

Cases Successfully Prosecuted: Aerojet Rocketdyne ($9M)

- The new Civil Cyber-Fraud Initiative will leverage the **False Claims Act**, a civil enforcement tool meant to address fraudulent conduct by companies to gain federal funds from programs and operations.
- *"We will use our civil enforcement tools to pursue companies, those who are government contractors who receive federal funds, when they fail to follow required cybersecurity standards — because we know that puts all of us at risk,"* said Deputy Attorney General Lisa Monaco.
- Companies that **knowingly delivered deficient cybersecurity offerings, misreported cybersecurity practices or protocols and compromised cyber attack monitoring and reporting will be held accountable** by the department as part of the initiative.
- DOJ seeks to enhance overall cybersecurity practices, strengthen cyber threat resilience and gain reimbursement from companies that did not meet their cybersecurity obligations.
- The fraud section of the Civil Division's Commercial Litigation Branch will lead the initiative, which is expected to also draw from DOJ's collaborative efforts with law enforcement partners, other federal agencies and subject matter experts.

FAQs

Will Prime Contractors and Subcontractors be required to hold the same CMMC Level?

"If contractors and subcontractors are handling the same type of FCI and CUI, then the same CMMC level will apply. In cases where the prime only flows down select information, a lower CMMC level may apply to the subcontractor."

Will my Organization Need to be Certified if it Does Not Handle CUI?

"DoD's intent under CMMC 2.0 is that if a DIB company does not process, store, or transmit Controlled Unclassified Information (CUI) on its unclassified network, but does process, store or handle Federal Contract Information (FCI), then it must perform a CMMC Level 1 self-assessment and submit the results with an annual affirmation by a senior company official into SPRS." (CMMC Model (defense.gov)

Plan of Actions and Milestones (POA&Ms)

"With the implementation of CMMC 2.0, the Department intends to allow companies to receive contract awards with a Plan of Actions and Milestones (POA&M) in place to complete some CMMC requirements. The Department's intent is to specify a baseline number of requirements that must be achieved prior to contract award, in order to allow a remaining subset to be addressed in a POA&M within a clearly defined timeline. The Department also intends to specify a small subset of requirements that cannot be on a POA&M in support of achieving a CMMC certification." (CMMC Implementation (defense.gov)

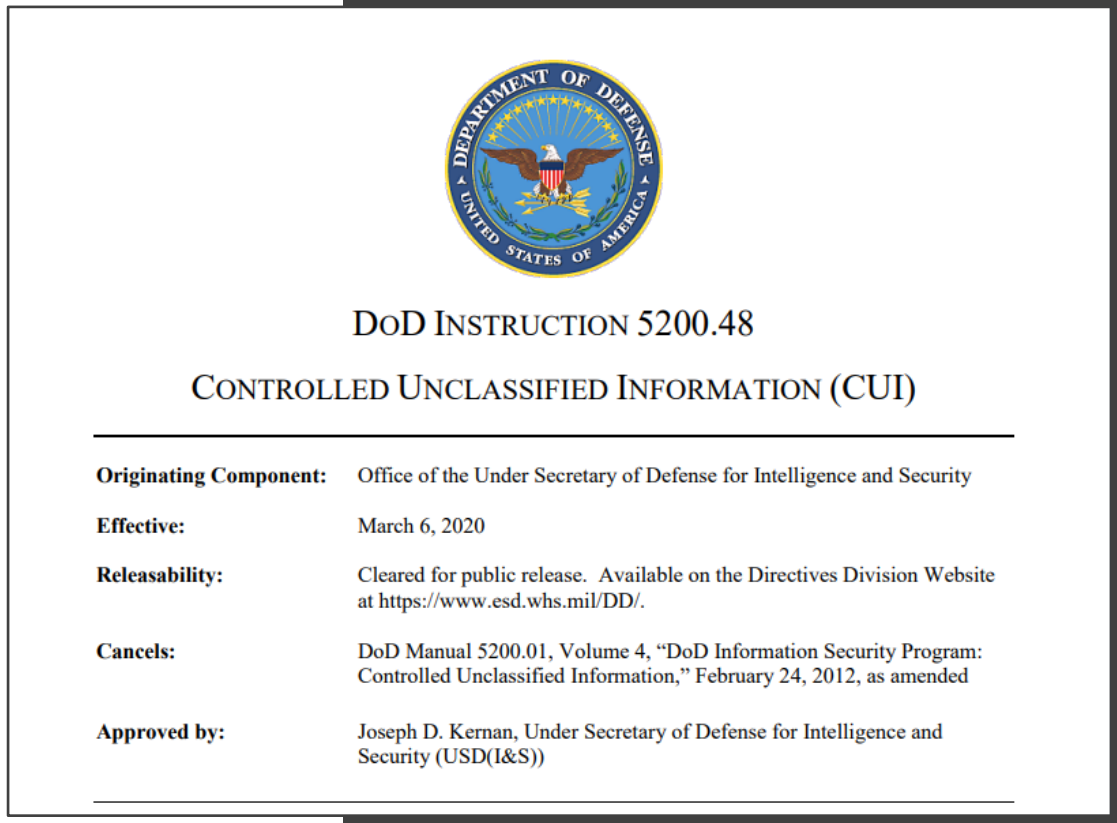
DoD Instruction 5200.48

DoD Instruction on Controlled Unclassified Information (CUI)

DoDI 5200.48

Controlled Unclassified Information (CUI)

- Establishes policy, assigns responsibilities, and prescribes procedures for CUI throughout the DoD in accordance with Executive Order (E.O.) 13556; Part 2002 of Title 32, Code of Federal Regulations (CFR); and Defense Federal Acquisition Regulation Supplement (DFARS) Sections 252.204-7008 and 252.204-7012
- Establishes the official DoD CUI Registry



DoD INSTRUCTION 5200.48

CONTROLLED UNCLASSIFIED INFORMATION (CUI)

Originating Component:	Office of the Under Secretary of Defense for Intelligence and Security
Effective:	March 6, 2020
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Cancels:	DoD Manual 5200.01, Volume 4, "DoD Information Security Program: Controlled Unclassified Information," February 24, 2012, as amended
Approved by:	Joseph D. Kernan, Under Secretary of Defense for Intelligence and Security (USD(I&S))

Source: DoDI 5200.48, "Controlled Unclassified Information (CUI)," Effective March 6, 2020 (whs.mil)

Disclosure of CUI

DODI 5200.48 - 5.3. REQUIREMENTS FOR DOD CONTRACTORS

- This paragraph highlights requirements for DoD contractors
  - Whenever DoD provides information to contractors, **it must identify whether any of the information is CUI via the contracting vehicle**, in whole or part, and mark such documents, material, or media in accordance with this issuance
  - Whenever the **DoD provides CUI to, or CUI is generated by**, non-DoD entities, protective measures and dissemination controls, including those directed by relevant law, regulation, or government-wide policy, **will be articulated in the contract, grant, or other legal agreement, as appropriate**

Marking CUI

HOW DO YOU KNOW WHEN TO MARK DATA AS CUI?

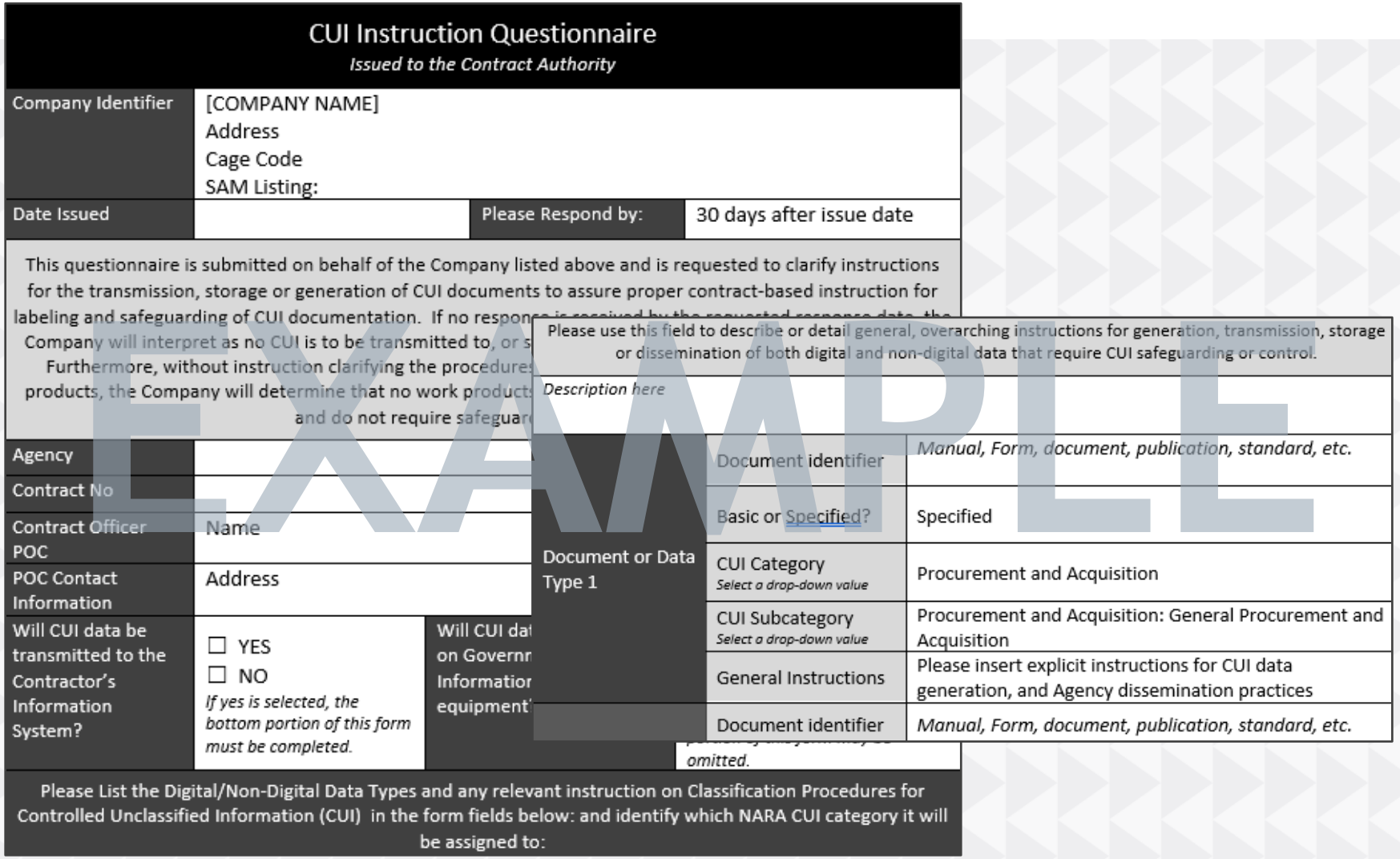
- Ask for a Security Classification Guide (SCG)
- Ask your Program's Contract Authority
  - They may provide you **written clarification** for each relevant contract for how generated data on the contract will be categorized
- Ask for "other document or memorandum"
  - Utilize a CUI Questionnaire
  - Ask CA to provide another document

Ask for a Security Classification Guide (SCG) for CUI

- DoDI 5200.48
  - 3.7. GENERAL DOD CUI REQUIREMENTS
    - "e. **CUI will be identified in SCGs** to ensure such information receives appropriate protection.
    - If the SCG is canceled, **a memorandum or other guidance document may be issued to identify CUI instead.**"

Memorandum or Other Guidance

EX: BDO CUI QUESTIONNAIRE



CUI Instruction Questionnaire

Issued to the Contract Authority

Company Identifier	[COMPANY NAME] Address Cage Code SAM Listing:		
Date Issued		Please Respond by:	30 days after issue date

This questionnaire is submitted on behalf of the Company listed above and is requested to clarify instructions for the transmission, storage or generation of CUI documents to assure proper contract-based instruction for labeling and safeguarding of CUI documentation. If no respon
Company will interpret as no CUI is to be transmitted to, or s
Furthermore, without instruction clarifying the procedures
products, the Company will determine that no work product
and do not require safeguar

Agency	
Contract No	
Contract Officer POC	Name
POC Contact Information	Address
Will CUI data be transmitted to the Contractor's Information System?	☐ YES ☐ NO *If yes is selected, the bottom portion of this form must be completed.*

Will CUI dat
on Governr
Informatior
equipment

Please use this field to describe or detail general, overarching instructions for generation, transmission, storage or dissemination of both digital and non-digital data that require CUI safeguarding or control.

Description here

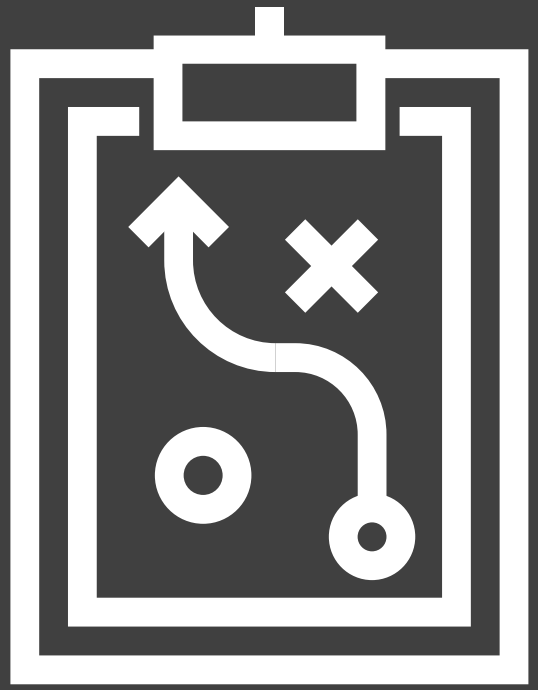
Document or Data Type 1	Document identifier	*Manual, Form, document, publication, standard, etc.*
	Basic or Specified?	Specified
	CUI Category *Select a drop-down value*	Procurement and Acquisition
	CUI Subcategory *Select a drop-down value*	Procurement and Acquisition: General Procurement and Acquisition
	General Instructions	Please insert explicit instructions for CUI data generation, and Agency dissemination practices
	Document identifier	*Manual, Form, document, publication, standard, etc.*

omitted.

Please List the Digital/Non-Digital Data Types and any relevant instruction on Classification Procedures for Controlled Unclassified Information (CUI) in the form fields below: and identify which NARA CUI category it will be assigned to:

EXAMPLE

Tips and Strategies for CMMC Compliance



Steps to CMMC Compliance

BDO'S METHODOLOGY FOR CMMC COMPLIANCE

1 SCOPE	1. Determine contract governance and CUI discovery 2. Mapping FCI and CUI in architecture, Use Cases 3. Define Authorization Boundaries
2 DESIGN & IMPLEMENT	4. Define Architectures for FCI and CUI 5. Scope technical solutions 6. Implement technical solutions
3 DOCUMENT	7. Create Policies/Procedures/Artifacts
4 ASSESS & VALIDATE	8. **Gap Assessment** 9. Verification & Validation (V&V)
5 CERTIFY	10. Certification (CMMC C3PAO)
6 MAINTAIN	11. Train, Test, Review & Update

TIPS & STRATEGIES FOR CMMC COMPLIANCE

First Stage: Scoping

SCOPING IS CRITICAL!

1. What do your contracts require? DFARS 252.204-7012, FAR 52.204-21, CMMC, CUI, ITAR?
2. What parts of your IT infrastructure does each data type touch?
3. How many users receive or generate CUI/ITAR?
4. Do you need to build a separate enclave to hold CUI separate from the enterprise?
5. Have you received a Security Classification Guide (SCG)?
6. Do you know which documents generated on a DoD program need to be marked by the organization as CUI?
7. Have you built a CUI Marking Registry for company-generated CUI documents?
8. How to you screen/vet personnel who need access to CUI
9. Do you have cyber training programs?

TIPS & STRATEGIES FOR CMMC COMPLIANCE

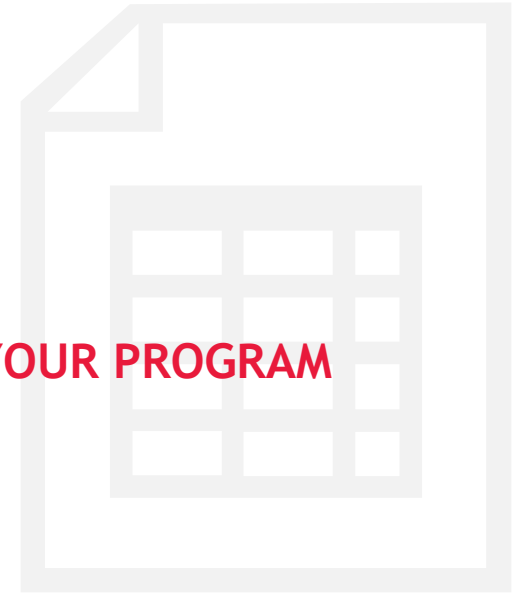
Second Stage: Design & Implement

ONCE YOU KNOW WHAT THE SCOPING STAGE LOOKS LIKE: NOW DESIGN & IMPLEMENT!

1. What is your Authorization Boundary (where CUI is transmitted, stored and processed in your IT systems and SaaS solutions)
2. What is your CUI Data flow between IT assets/solutions
3. Use Cases: What assets do the employees need to be operational AND process CUI?
4. Design IT architecture and solutioning to fit use cases
5. Deploy solutions
6. Secure areas of facility where CUI is processed
7. Train PMs and users how to access CUI and how to safeguard it

TIPS & STRATEGIES FOR CMMC COMPLIANCE

Third Stage: Document



NOW THAT YOU HAVE IMPLEMENTED YOUR COMPLIANT ARCHITECTURE: DOCUMENT YOUR PROGRAM

1. Policies & Procedures for:
   a. NIST 800-171 Non-Federal Organization (NFO) Controls
   b. NIST 800-171/CMMC Level 1 controls (affects FCI)
   c. NIST 800-171/CMMC Level 2 controls (affects CUI)
2. Systems Security Plan (SSP) - security roadmap for safeguarding CUI against NIST 800-171 controls.
3. Plan of Actions & Milestones (POAM) – what you have implemented and what is still unimplemented, plus timeline for implementation of control.
4. Incident Response Plan (IRP) – detailed information for what you will do in the event of an incident and how to investigate, triage, mitigate/remediate and report it to DIBnet within 72 hours of discovery.
5. BDO has template repository of over 55 documents to satisfy your CMMC readiness package

TIPS & STRATEGIES FOR CMMC COMPLIANCE

Fourth Stage: Assess & Validate

AFTER FULL DOCUMENTATION STAGE

1. Collect a minimum of 2 pieces of evidence per control (cover all objectives for each control) - Note: Assessors may ask for more than 2
2. Review SSP, POAM, and policies and procedures
3. Perform final Gap Assessment
4. Close out any gaps found, POAM what cannot be remediated.
5. Perform Validation by reviewing and validating 2 pieces of evidence per control.
   - Evidence list can be found in the CMMC Assessment guide for CMMC 2.0 Level 2.
   - CMMC CAP (C3PAOs instruction manual) marks that 80% of controls must be satisfied for CMMC certification. (Weighted 5 and 3 controls must be satisfied).

CMMC Certification

What You Need to Know Before Contracting with a C3PAO

Be Prepared and Then Reach Out to an Authorized C3PAO

- Have a Gap Assessment completed by a certified CMMC RPO or C3PAO
- Select Authorized C3PAO(s) at the CMMC Marketplace at CyberAB
- Obtain a Proposal from your selected C3PAO(s)
- Choose your C3PAO to get in the queue for a Joint Assessment
- C3PAO will submit for approval with DIBCAC (now you're in DIBCAC's queue)
- The C3PAO will coordinate your assessment once the pre-assessment coordination meeting is scheduled by the DIBCAC
- The C3PAO and DIBCAC will jointly perform the assessment. The DIBCAC will upload results to eMASS
- Once certified, it will be posted to SPRS and can be authorized for 3 years
- Remember NIST 800-171 has been a requirement since 2015 – all contractors should have been compliant by December of 2017

DO NOT WAIT

Joint Voluntary Assessments Began in August of 2022

The Joint assessment team typically consists of approximately 2-4 assessors from the C3PAO and assessors from the DCMA DIBCAC team. 4 weeks before the on-site assessment the team will meet virtually via a pre-assessment coordination meeting with the OSC. This will be followed by a thorough review of the SSP and all supporting documentation.

The on-site assessment begins after the documentation review stage is passed with a kickoff meeting, where the team will review the schedule for each day of the assessment. The assessors will request to observe your controls in action and inquire about settings for key applications and policies. Some assessments are still done virtually.

Applicable interviews will be requested with the Systems Administrators or MSPs supporting your enclave, but will also include interviews with Human Resources, Facility Security, Chief Information Officer (CIO), Chief Information Security Officer (CISO), Stakeholders/C-Suites, and many potential other personnel that have an active role assigned within the control families of NIST 800-171.

The scope of the assessment will be determined by the environment scope you provide to the C3PAO. This is called an Authorization Boundary. This controlled boundary may include the following data:

- Federal Contract Information (FCI)
- Controlled Unclassified Information (CUI)
- Legacy CUI includes FOUO, OUO, SBU, LES, and DoD Technical Data (CTI/UCTI)
- Export Controlled Data (ITAR/EAR)

Frequently Asked Questions

- What if you have open POAM items?
- Can you close out open POAM items while the assessor is still performing the assessment?
- How many controls to pass a certification?
- Are some controls more important to close out than others?
- How do I know which controls are critical and which can be POAM'ed?
- What if I fail the assessment?
- Can you do a pre-assessment before the final certification, so I know if my organization is ready?

What Is the Typical On-Site Schedule for An Assessment

NIST/CMMC ASSESSMENT

Day 1

ID & Access Management

- Access Control
- Audit & Accountability
- Identification & Authentication

Day 2

Cyber Security Oversight & Management

- Awareness & Training
- Personnel Security
- Physical Protection
- Risk Assessment
- Security Assessment

Day 3

Configuration Management

- Configuration Management
- Maintenance
- Media Protection

Day 4

Network Defense

- Incident Response
- Systems & Communications
- System & Information Integrity

TBD

Deliverables

- Final Assessment Report

Questions?

Thank You!

CHRISTINA REYNOLDS

Industry Specialty Services Director

256-998-8093
creynolds@bdo.com

EXPERIENCE

Christina is a Cybersecurity Maturity Model Certification (CMMC) Registered Practitioner (RP) with 22 years of specialization in cybersecurity and information assurance policy, including application and guidance for DoD contractors in support of CMMC, DFARS 252.204-7012, NIST 800-171, NIST 800-172, NIST 800-53, HIPAA, CFPB, PCI, CIS, EXOSTAR, DCSA RMF packages, and other industry-mandated cybersecurity regulations.

Christina has served as a senior systems engineer and ISSO supporting multiple DoD BMDS programs under U.S. Army, U.S. Navy/NAVWAR, and MDA programs, as well as more than 150 commercial IT and cyber customers. She has provided thought leadership for the IT and cyber sectors, including two published books, “Zen and the Art of DFARS 7012 Compliance” and “Weather the Storm in the Cloud: Maintaining Active DFARS 7012 Compliance in the Cloud.”

Previously serving as executive CEO of a defense contractor, she led a consulting IT and cybersecurity team, providing program management, business development, government contract management, technical proposal development, and GSA schedule management, as well as leading program management for MDA, U.S. Navy/NAVWAR, and U.S. Army contracts and subcontracts supporting Army tactical elements.

CERTIFICATIONS

- EC-Council Certified Ethical Hacker
- EC-Council Certified Hacking Forensic Investigator
- EC-Council Certified Network Defense Architect

EDUCATION

- B.S. Materials Science and Engineering, Penn State University
- M.S. Cybersecurity and Information Assurance, Western Governors University

STACY HIGH-BRINKLEY

Industry Specialty Services Group
Senior Manager

540-220-5963
shighbrinkley@bdo.com

EXPERIENCE

Stacy High-Brinkley has more than 30 years' experience as an Information Security professional. Her background includes building and securing networks, with expertise in establishing and implementing streamlined cyber security programs. She holds numerous Cyber Certifications and is also a certified CMMC Certified Assessor (CCA) as well as an RMF Assessor for DoD. Her expertise of the cyber domain includes technical aspects such as ensuring proper implementation of security controls and hardening networks as well as non-technical and policy implementation. Her passion is working with others, enabling a positive, environment and learning new ways to create secure environments in our hyper connected world.

Stacy has worked in wide ranging positions throughout her career, most recently serving as the Chief Information Security Officer (CISO) for a defense contracting company.

CERTIFICATIONS

- Cyber-AB: Certified CMMC Assessor (CCA)
- Cyber AB: Provisional Assessor (PA)
- Certified CMMC Professional
- CISSP
- CNSS Risk Analyst
- CNSS System Certifier
- DoD Licenses: Marine Corps Validator, Navy Validator
- AXELOS - Information Technology Infrastructure Library (ITIL)
- AXELOS – Resilia Foundations

EDUCATION

- B.A. Psychology & Sociology, Shepherd College

BDO GovCon Cyber Team

Years Exp

CHRISTINA REYNOLDS
Director | Program Manager

MS Cybersecurity & Information Assurance
BS Materials Science & Engineering

Certifications: CMMC RP, Certified Ethical Hacker (CEH) | Certified Hacking Forensic Investigator (CHFI)| Certified Network Defense Architect (CDNA)

STACY HIGH-BRINKLEY
Sr Manager | PM/Validator

CMMC Certified Assessor (CCA)
BA, Psychology & Sociology

Certifications: ISC^2 Certified Information Systems Security Professional (CISSP) | Navy/Marine Corps Validator | CNSS Risk Analyst |

AUSTIN FLANNERY
Sr. Manager | PM/Validator

PhD Cyber Policy
BS Cybersecurity
MS MBA
AS Network Security

Certifications: CMMC RP, CompTIA Security +, CISM, NQV Navy/Marine Corps Validator

ANDREW ZOPPI
Manager | Systems Architect

MS, Cybersecurity
BS, Data Networking & Info Sec
AS, Applied Science
Und. Cert: Management Foundations

Certifications: GIAC Public Cloud Security (GPCS), GIAC Cloud Security Essentials (GCLD), (ISC)2 Certified Information Systems Security Professional (CISSP), + 6 CompTIA Certs

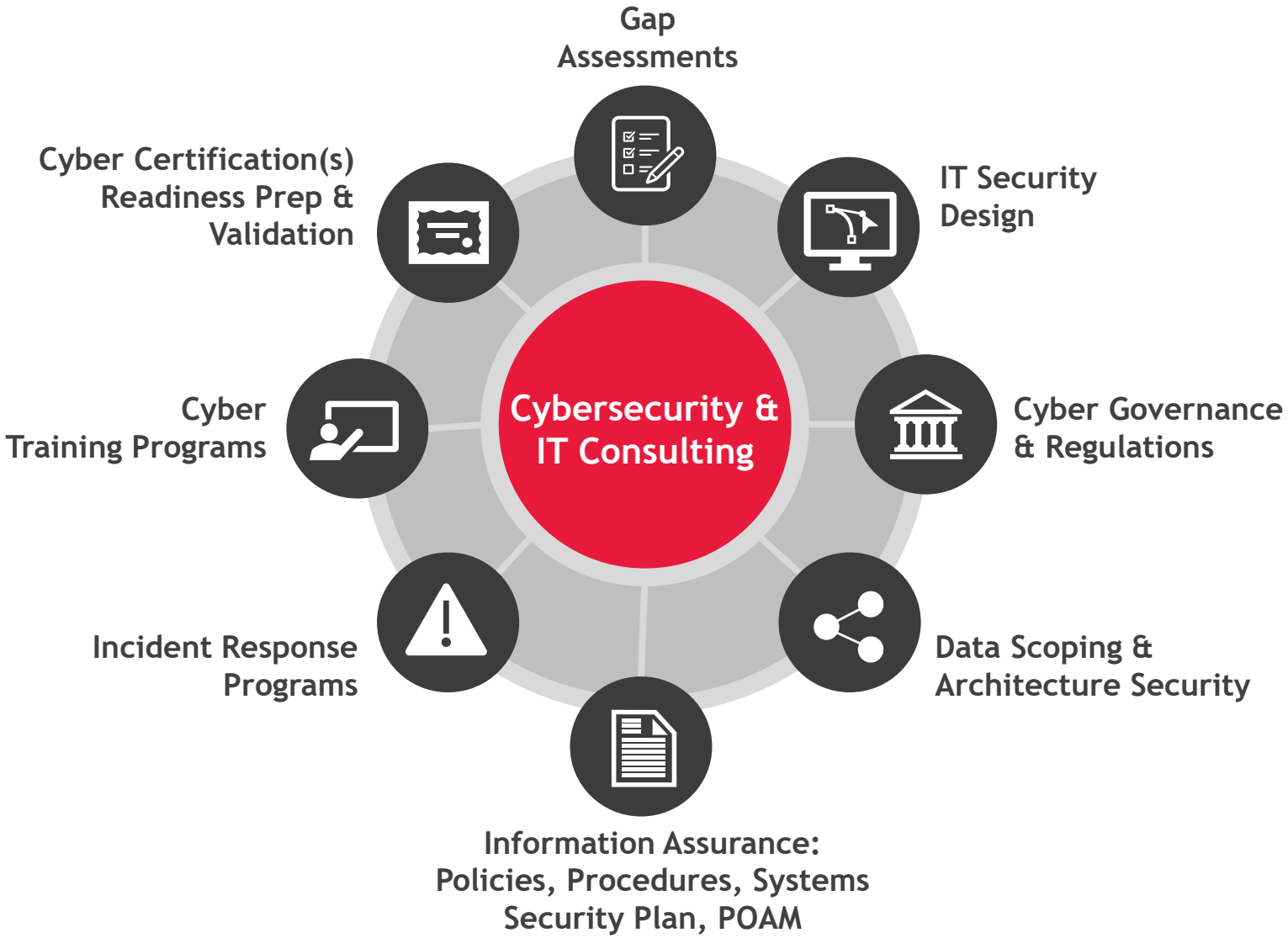
LINDSEY ROBERTSON
Sr. Associate | ISSM

BA Geography – Minor GIS
AS General Studies

Certifications: CMMC RP, CompTIA Sec +

Cybersecurity & IT Systems Design

SECURITY. ASSURANCE. COMPLIANCE.



Cybersecurity & IT Systems Design

SECURITY. ASSURANCE. COMPLIANCE.

The increased threat landscape has brought about an era of ever-increased vigilance towards cybersecurity governance, regulations and security design. BDO can quickly develop a plan and course of action to enhanced IT security, whether you need help with strategy, design, implementation, or ongoing operations. Navigate your most critical business and mission operations, incorporate pertinent governance and regulatory requirements, and build a strong defense-in-depth cyber program to position your organization to be more robust, resilient and proactive to the threat landscape.

BDO's Cybersecurity Specialists provide a practiced and scalable approach to building robust and resilient IT architectures that tailor to your organization's operations. Our cyber specialist team respond flexibly to meet new threats and vulnerabilities, build a comprehensive cybersecurity program for resilience, and leverages cyber experience with global knowledge, offering a one-stop, cost-effective service for cybersecurity strategy.

Cybersecurity & IT Systems Design

SECURITY. ASSURANCE. COMPLIANCE.

CREDENTIALED CYBER SPECIALISTS

- IT & Cybersecurity Professionals with advanced degrees, certification and experience
- Knowledgeable in multiple cybersecurity frameworks to fit your business mission and operations

INFORMATION ASSURANCE PROGRAMS

- Robust sets of policy & procedures templates to meet any regulation or governance structure
- Knowledgeable in security design to help create a tailored Systems Security Plan and POAM

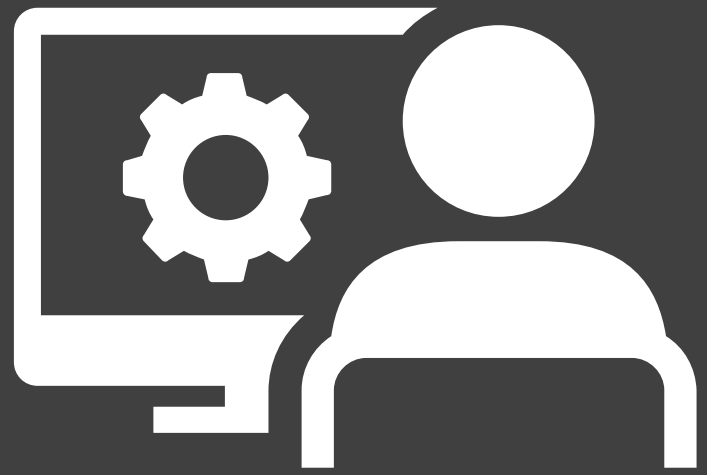
TECHNOLOGY AGNOSTIC

- Practiced security architecture strategies with market-leading IT platforms and solutions
- Flexible to incorporation of existing technologies within the environment
- Analysis of regulations and governance to meet use-case scenarios
- Cloud-based design strategies for flexible deployments to business operations

FOCUSED DESIGN STRATEGIES FOE BUSINESS AND MISSION

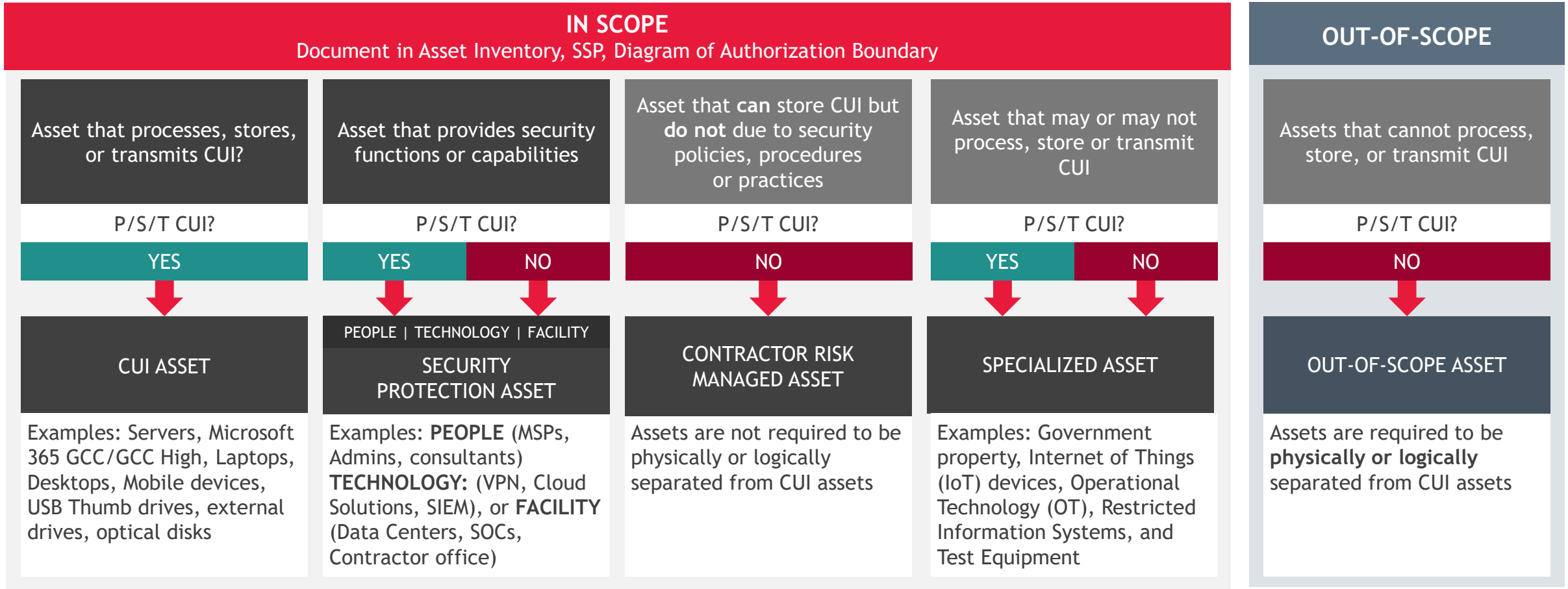
- Cybersecurity consulting strategies that can scale to meet business & mission operations
- Cybersecurity services are tailored to risk/threat analysis

Extra Slides



CMMC 2.0

Scoping the Environment for CUI Assets

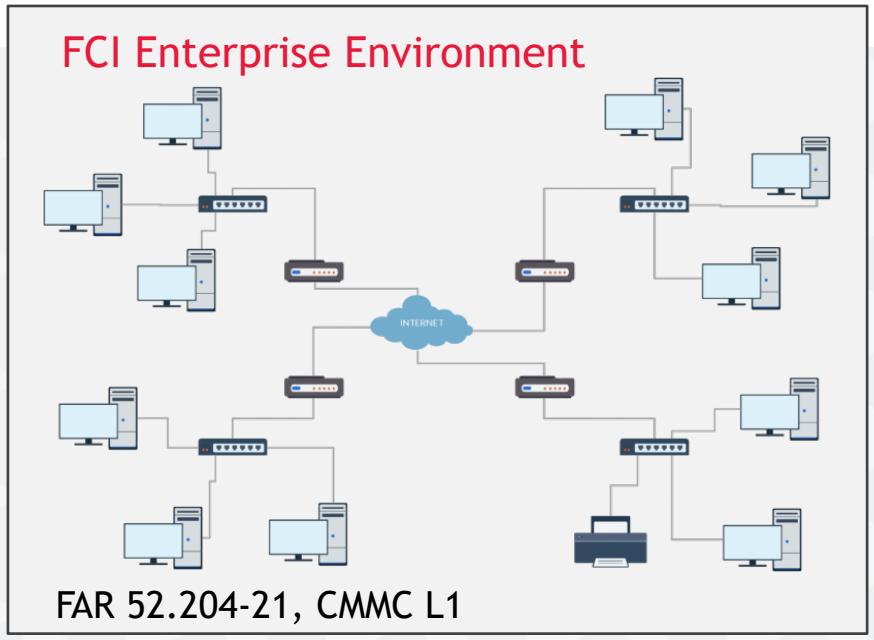


TASK 3

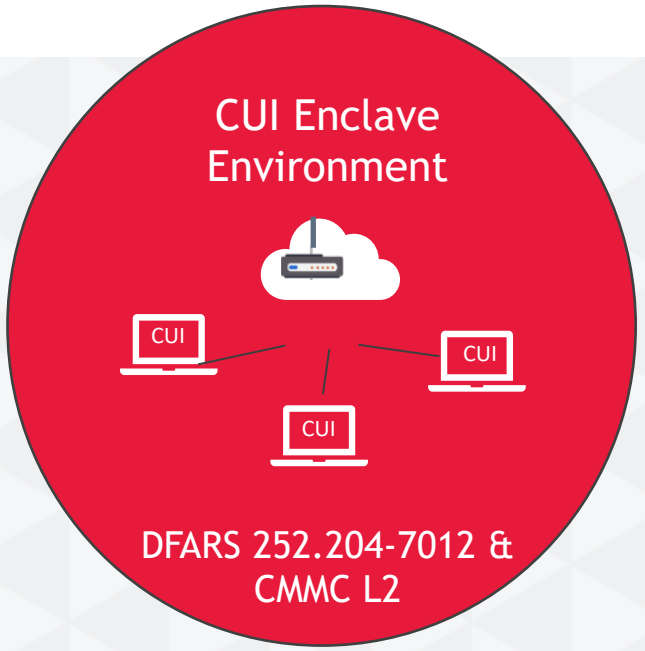
Define Authorization Boundaries

Determine the authorization boundaries for 1) FCI and 2) CUI environments, including all computing resources, network resources, software and personnel.

FCI Authorization Boundary



CUI Authorization Boundary



CUI Data Flow

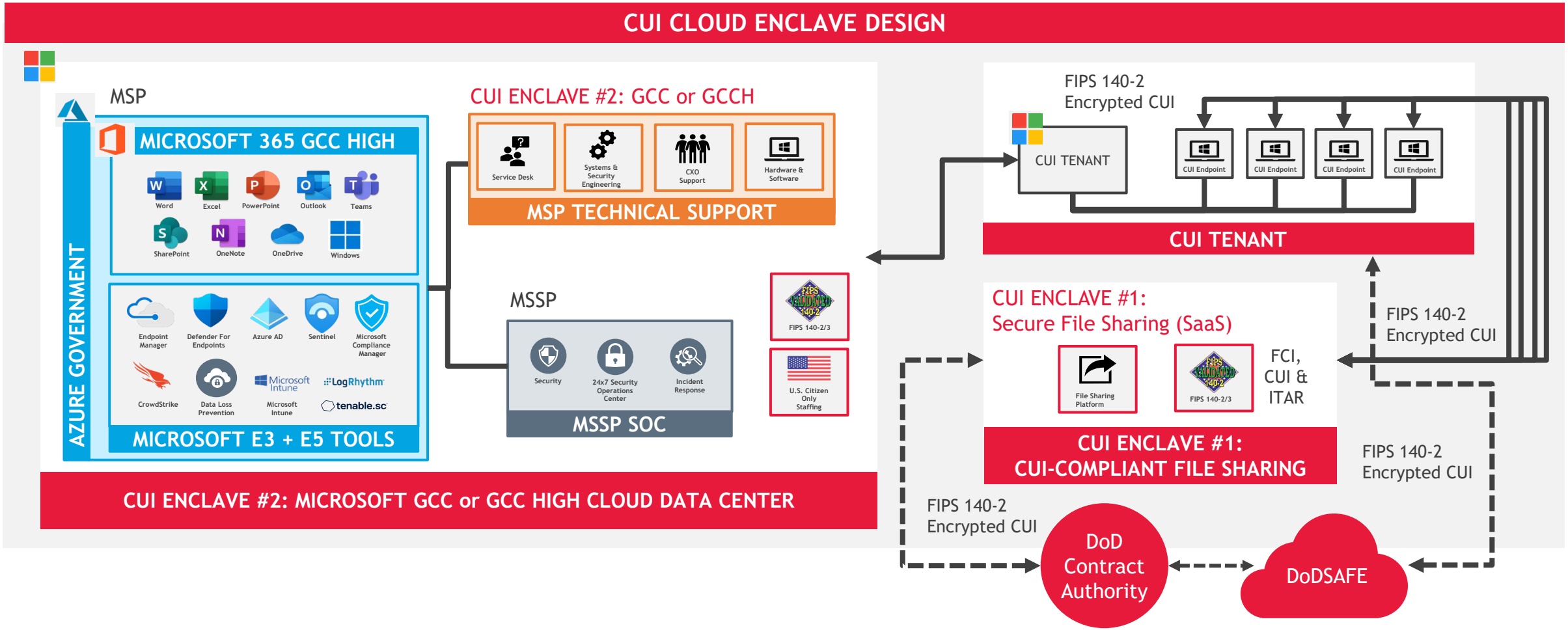
CUI-COMPLIANT CLOUD ENVIRONMENT ARCHITECTURAL OVERVIEW

2 SOLUTIONS

1. Primary Laptop Enterprise/Secondary Laptop GCCH
2. Windows365 (GCCH is not released yet BUT)
   a. ***Option 1: Windows 365 Commercial on GCCH laptop (more secure)
   b. Option 2: Windows365 GCCH on Commercial/Enterprise

CUI Data Flow

CUI-COMPLIANT CLOUD ENVIRONMENT ARCHITECTURAL OVERVIEW



Microsoft 365 Government (DoD)

	Commercial	M365 "GCC"	M365 "GCC High"	M365 "DoD"
Customer Eligibility	Any customer	Federal, SLG, Tribes, DIB	Federal, DIB	**DoD only**
Datacenter Locations	US & OCONUS	CONUS Only	CONUS Only	**CONUS Only**
FedRAMP *	High	High	High	**High**
DFARS 252.204-7012	No	Yes	Yes	**Yes**
FCI + CMMC L1-2	Yes	Yes	Yes	**Yes**
CUI / CDI + CMMC L3-5	No	Yes^	Yes	**Yes**
ITAR / EAR	No	No	Yes	**Yes**
DoD CC SRG Level **	N/A	IL2	IL4	**IL5**
NIST SP 800-53 / 171 ***	Yes	Yes	Yes	**Yes**
CJIS Agreement	No	State	Federal	**No**
NERC / FERC	No	Yes^	Yes	**Yes**
Customer Support	Worldwide / Commercial Personnel		US-Based / Restricted Personnel	
Directory / Network	Azure Commercial		Azure Government	
			US Sovereign Cloud	

* *Equivalency,* Supports accreditation at noted impact level

** *Equivalency,* PA issued for DoD only

*** Organizational Defined Values (ODV's) will vary

^ CUI Specified (*e.g. ITAR, Nuclear, etc.*) not suitable REQS US Sovereignty

About BDO USA

At BDO, our purpose is helping people thrive, every day. Together, we are focused on delivering exceptional and sustainable outcomes — for our people, our clients and our communities. Across the U.S., and in over 160 countries through our global organization, BDO professionals provide assurance, tax and advisory services for a diverse range of clients.

BDO is the brand name for the BDO network and for each of the BDO Member Firms. BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms.

www.bdo.com