



What to Expect in a CMMC Assessment Part II

LESSONS FROM A CMMC C3PAO

JUNE 21, 2023

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.

BDO[®]

With You Today



CHRISTINA REYNOLDS
Industry Specialty Services
Director, CMMC Registered
Practitioner (RP),
CEH, CHFI, CNDA

256-733-1115
creynolds@bdo.com



STACY HIGH-BRINKLEY
Industry Specialty Services
Sr Manager, Certified CMMC
Assessor (CCA), CISSP

540-220-5963
shighbrinkley@bdo.com



ERIKA PRIMMER
Director, Risk &
Compliance, CMMC Lead,
Cask Government Services

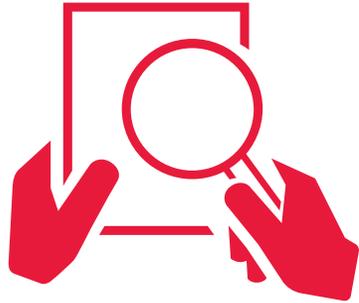
erika.primmer@caskgov.com



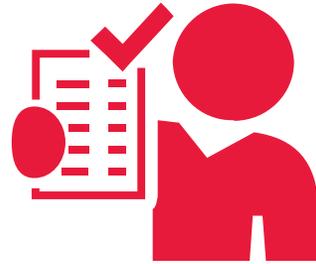
ROSE KINGOMBO
Systems Integrity &
Recovery, CCB Chair, Cask
Government Services

rose.kingombo@caskgov.com

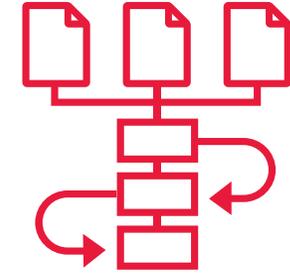
Learning Objectives



Recognize when to expect CMMC 2.0 rulemaking to be finalized and reflected in contracts



Identify changes from the NIST 800-171 Rev 3 draft release and its affect on compliance package for CMMC and future assessments



Apply tips and strategies for CMMC Assessment with a C3PAO/Joint Surveillance Assessment, including preparation and comparison of document reviews, interviews, and application of practices.

Agenda for Today

1	About FCI and CUI Clauses
2	CMMC
3	CMMC Rulemaking
4	Tips and Strategies for CMMC Compliance
5	CASK-chat
6	CMMC Certification: What You Need to Know Before Contracting with a C3PAO
7	Questions

About FCI and CUI Clauses



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

Federal Contract Information (FCI)

DEFINITION	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. Applies to Commercial items (including services).
EXEMPTION	<ul style="list-style-type: none">▶ Federal contract information does not include “simple transactional data” (e.g., for billing or payment processing) or information intended for public release (e.g., publicly accessible website data).▶ Not applicable to commercially available off-the-shelf (COTS) (e.g., printers, copiers) items.▶ Still applies to Commercial Items
FLOW DOWN	Mandatory flow down to subcontractors
MARKING	There are no current formal markings for FCI

Reference: [FAR 52.204-21](#)

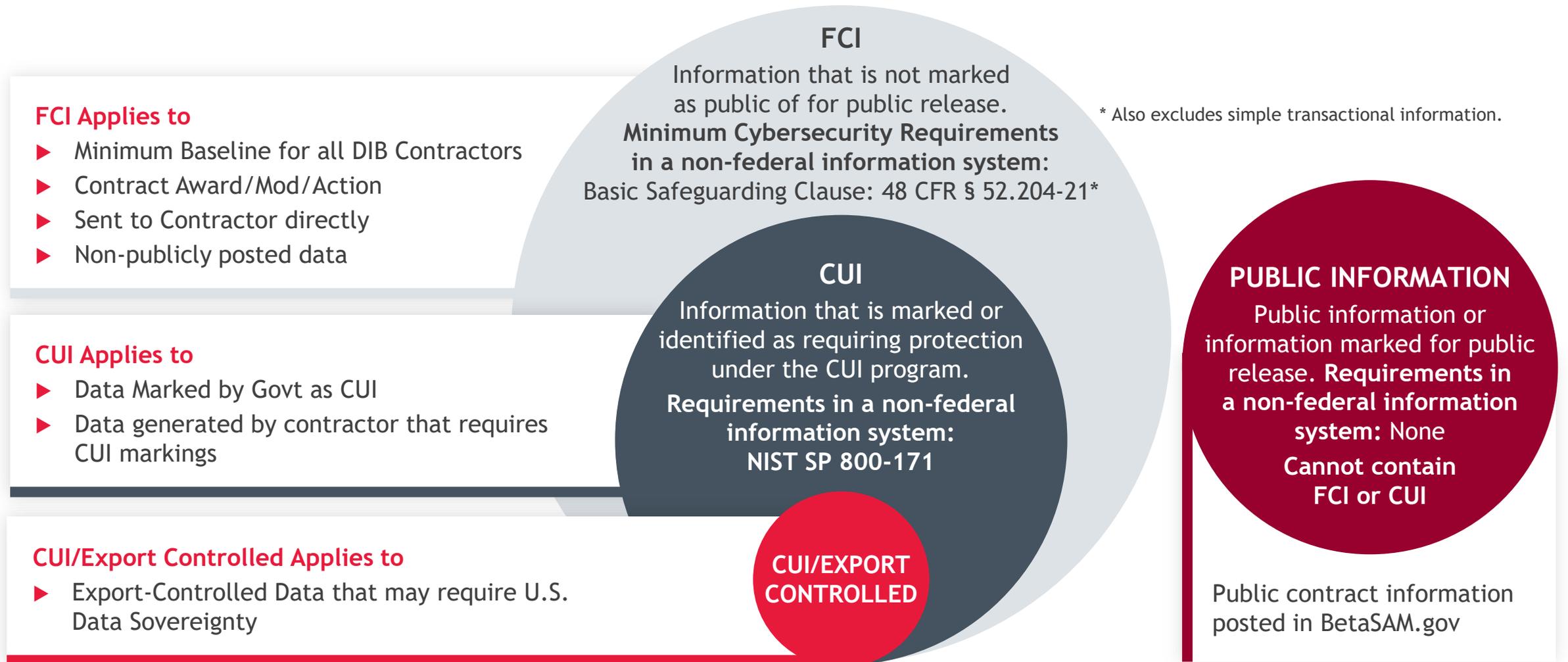
Examples of federal contract information include:

- ▶ Contract Information
- ▶ Contract Award/Mod/Option
- ▶ Emails exchanged between the DoD and defense contractor
- ▶ Proposal responses
- ▶ Contract performance reports
- ▶ Organizational or programmatic charts
- ▶ Process documentation
- ▶ Past performance information

Does not include:

- ▶ COTS Items
- ▶ Simple transactional data
- ▶ Information intended for public release

FCI & CUI Venn Diagram



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

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 -205-110.
- ▶ 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 (exl. COTS)

DFARS 252.204-7024

- ▶ SPRS scores are incorporated into supplier risk assessments
- ▶ Inaccurate SPRS scores could open contractors to legal risk, including False Claims Act (FCA) liability

Controlled Unclassified Information (CUI)

DEFINITION	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
EXEMPTION	Commercial products and commercial services
FLOW DOWN	Mandatory flow down to subcontractors for which subcontract performance will involve covered defense information , including subcontracts for commercial products or commercial services.
MARKING	Basic or Specified CUI markings, see NARA CUI List

Reference: [DFARS 252.204-7012](#)

Technical Information Examples:

- ▶ 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
- ▶ computer software executable code and source code

Does not include:

- ▶ Commercial Products
- ▶ Commercial Services

CUI Basic, CUI Specified, or Both?

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

1

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.

2

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

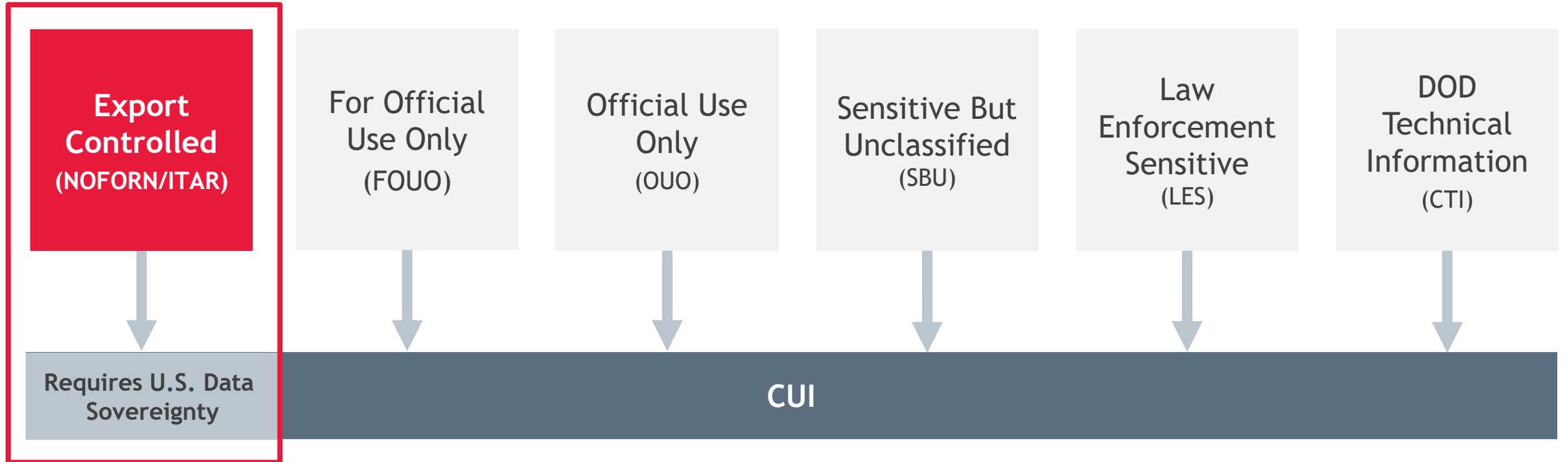
3

CUI SPECIFIED (but with CUI Basic controls)

Where the advisor 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 advisor does not specify.

What Is CUI?

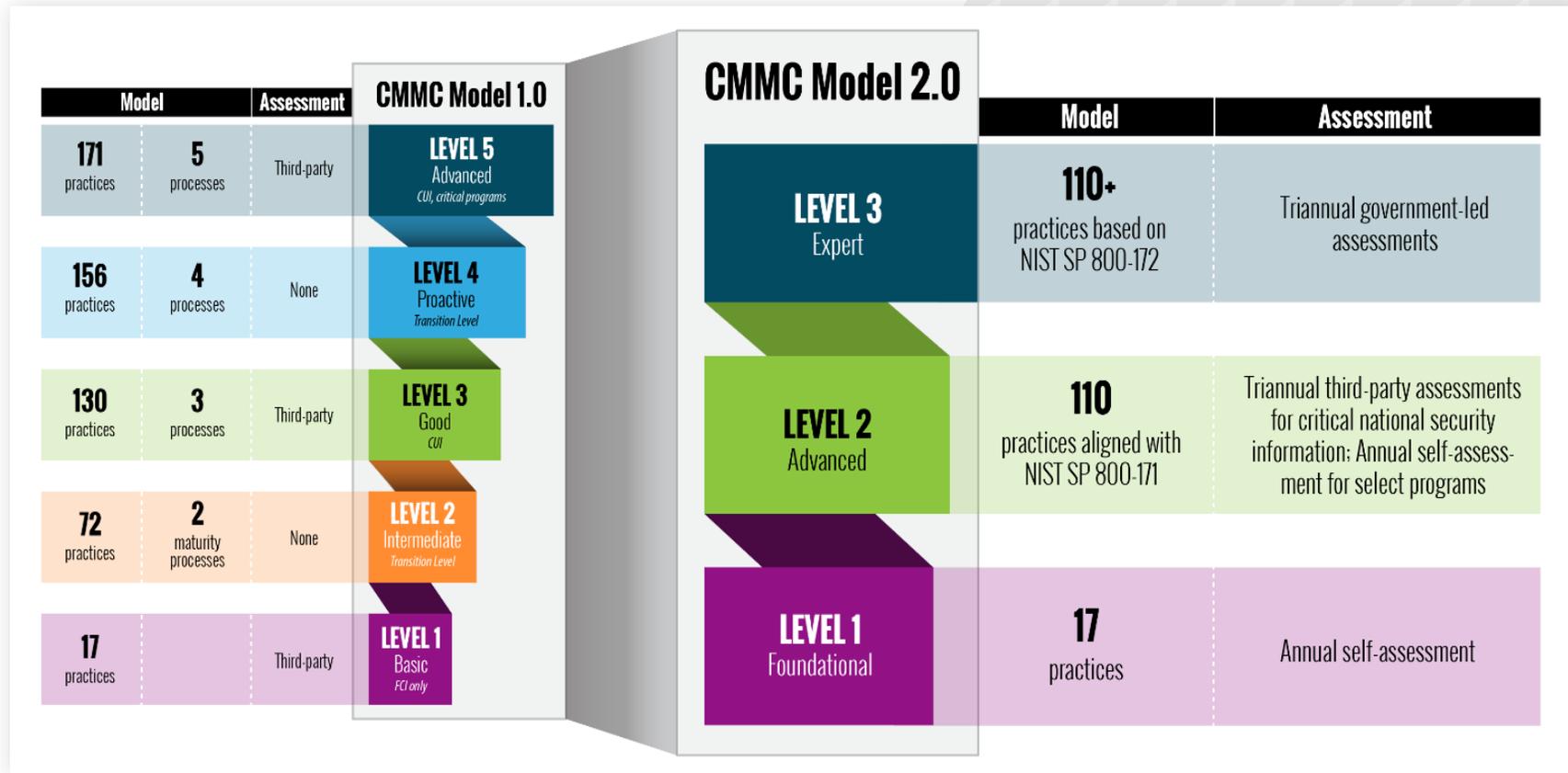
HOW DO YOU KNOW IF CUI DATA IS ALREADY ON YOUR SYSTEMS?



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

CMMC

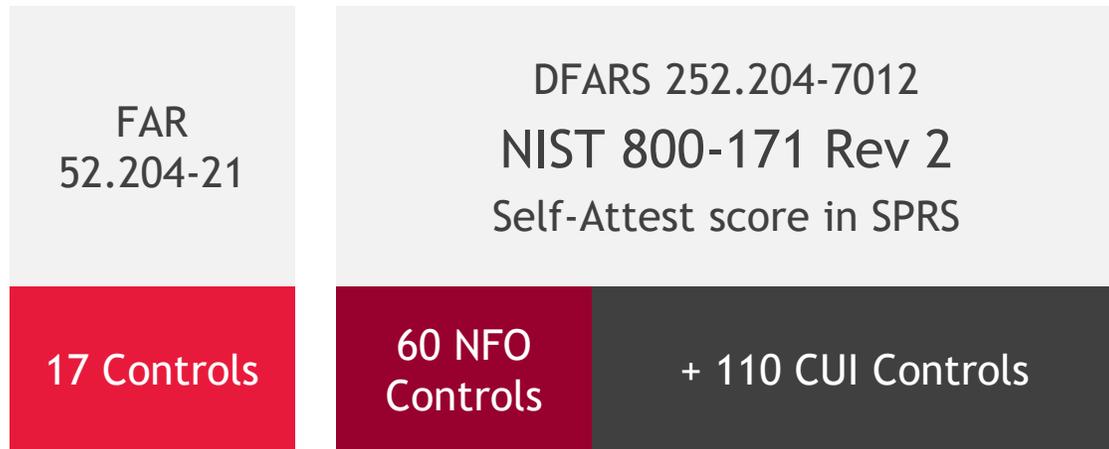
CMMC 2.0 Processes



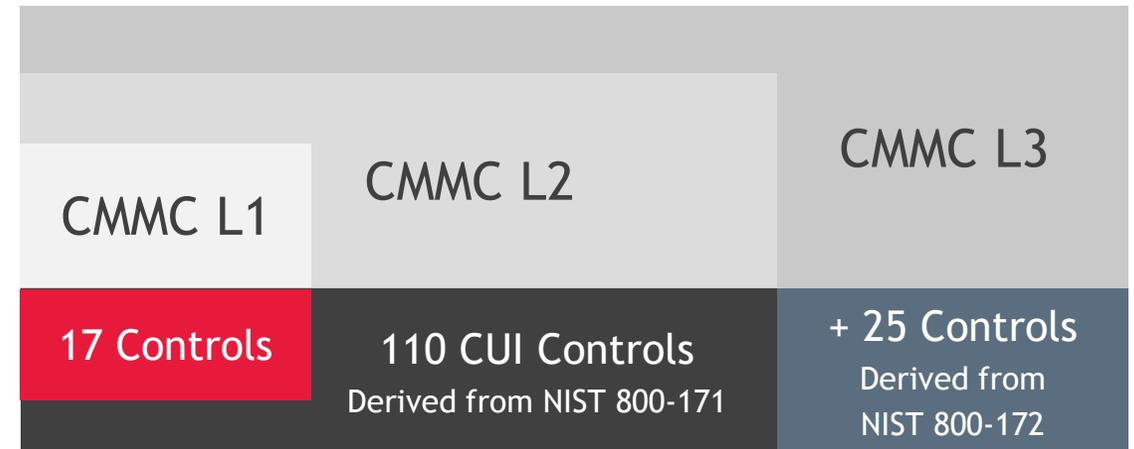
Source: [CMMC Model \(defense.gov\)](https://www.defense.gov/cmmc-model)

Security Controls and Inheritance Between Frameworks

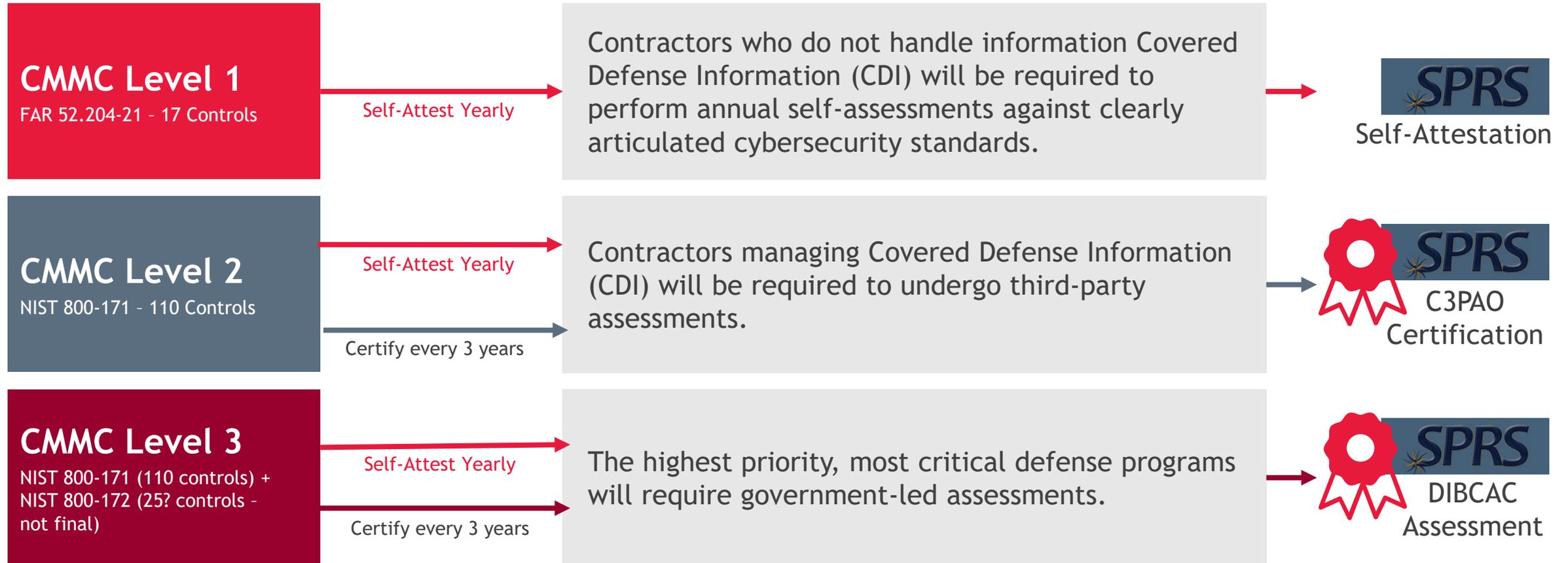
IN YOUR CONTRACTS NOW



WILL BE IN CONTRACTS BY 2025



Overview of CMMC 2.0 Assessments



CMMC Rulemaking

Information You Should Know
Regarding the CMMC 2.0 Final Rule



Latest on CMMC Rule Making

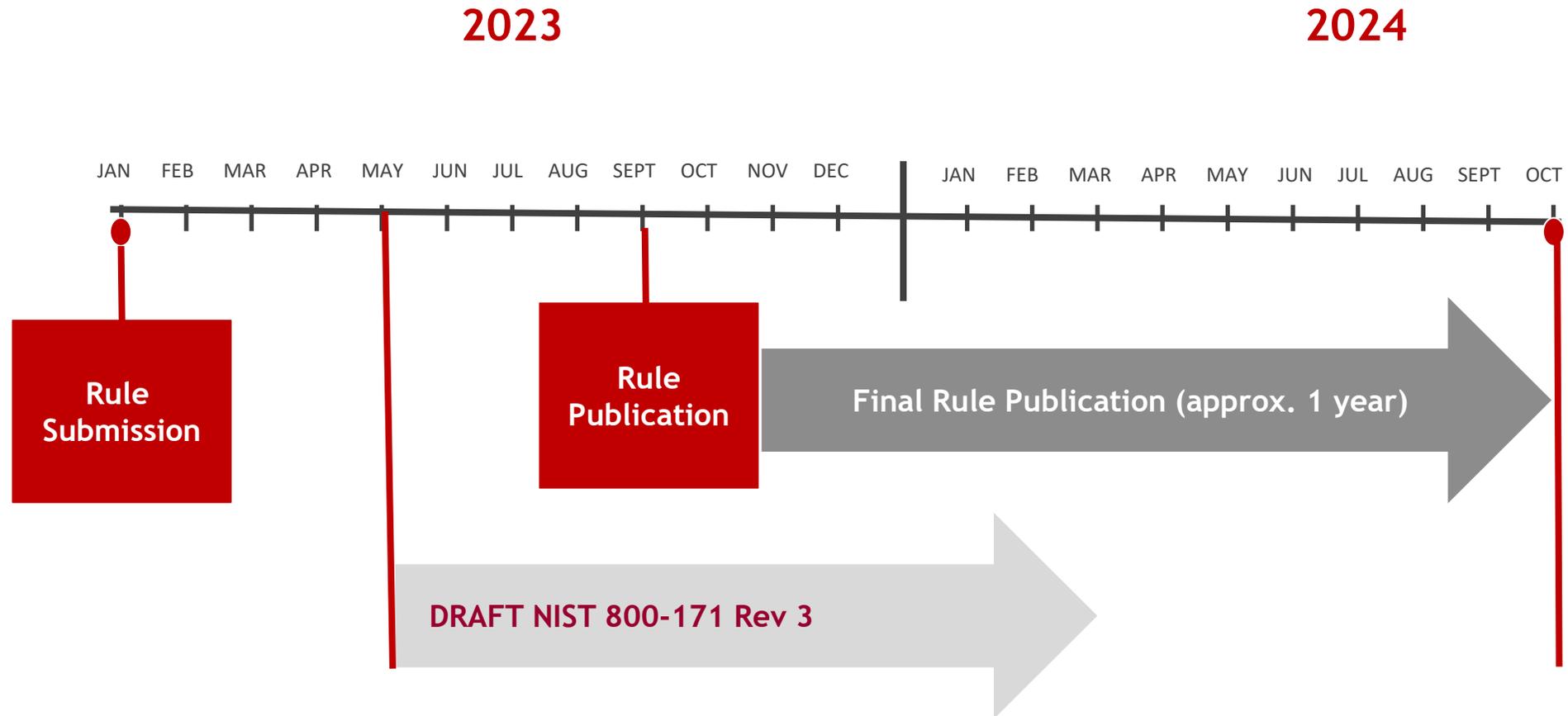
Rule Making

- ▶ The rulemaking process and timelines can take up to 24 months. CMMC 2.0 will become a contract requirement once rulemaking is completed
- ▶ Spring Agenda Published: 13 June 2023
- ▶ Proposed Rule: September 2023
[DASHBOARD - REGINFO.GOV](https://www.reginfo.gov/public/default.aspx?ref=647021)

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 \(reginfo.gov\)](https://www.reginfo.gov)

DoD Public Comments in May 2023

“We Still don’t have CMMC 2.0 out of the building yet because we’re working to get it right. It’s going to go to the Small Business Administrations first and then into [the Office of Management and Budget] here in the hopefully very near future...rest assured we want to get this right.”

— Hon. John Sherman, CIO, Department of Defense
May 16th

“We’re targeting late fall of next year, so that [CMMC] can start to be put into contracts.”

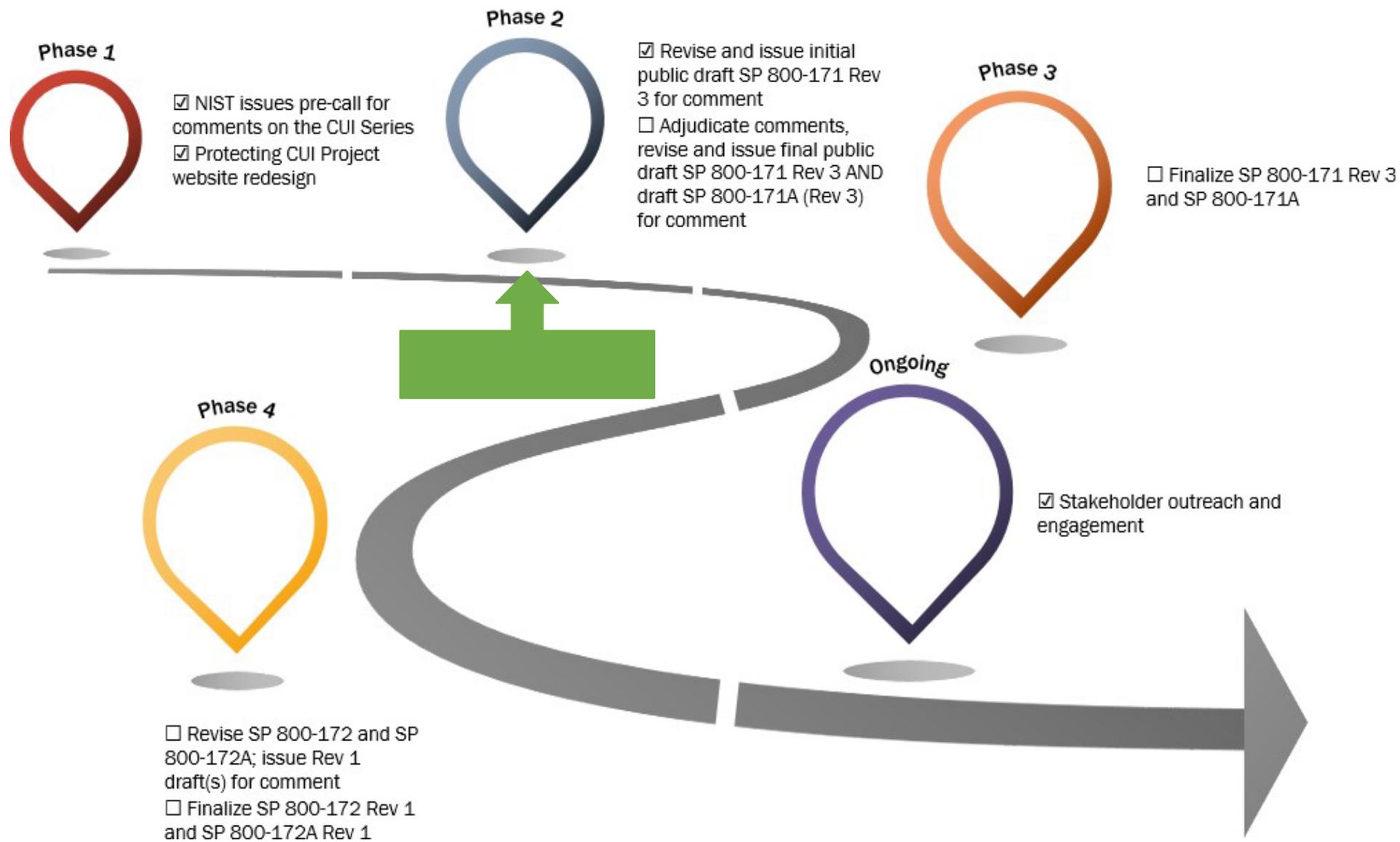
— David McKeown, CISCO and Deputy CIO, Department of Defense
May 18th

DRAFT NIST 800-171 Rev 3 Security Requirements

Draft SP 800-171 Rev 3 Security Requirement Families			
Access Control (Added: 1, Withdrawn: 5)	Maintenance (Added: 0, Withdrawn: 3)	Security Assessment & Monitoring (Added: 3, Withdrawn: 1)	
Awareness & Training (Added: 0, Withdrawn: 0)	Media Protection (Added: 0, Withdrawn: 2)	System & Communications Protection (Added: 2, Withdrawn: 4)	
Audit & Accountability (Added: 0, Withdrawn: 0)	Personnel Security (Added: 0, Withdrawn: 0)	System & Information Integrity (Added: 1, Withdrawn: 3)	
Configuration Management (Added: 0, Withdrawn: 1)	Physical Protection (Added: 2, Withdrawn: 3)	New Families	Planning (Added: 4)
Identification & Authentication (Added: 1, Withdrawn: 4)	Risk Assessment (Added: 1, Withdrawn: 1)		System & Services Acquisition (Added: 2)
Incident Response (Added: 0, Withdrawn: 0)			Supply Chain Risk Management (Added: 4)

- ✓ Aligned with SP 800-53 Rev 5 and SP 800-53B Moderate Baseline
- ✓ No change in total number of requirements (still 110)

Timeline for the CUI Series from NIST



Should You Wait?

THERE IS A LOT TO DO

120
Days

Phase 1

- ▶ Request Assessment
- ▶ Establish Roles and Responsibilities
- ▶ Organize and Prepare Assessment Documentation
- ▶ Ascertain Assessment Conditions and Requirements
- ▶ Complete Pre-Assessment Planning
- ▶ Verify Readiness to conduct the assessment

5
Days

Phase 2

- ▶ Assessment Kickoff Meeting
- ▶ Collect and Examine Evidence
- ▶ Score practices and validate preliminary results
- ▶ Generate and validate recorded findings

10
Days

Phase 3

- ▶ Deliver Recommended assessment results
- ▶ Submit package
- ▶ Archive assessment documentation

180
Days

Phase 4

- ▶ Perform POA&M and close out assessment
- ▶ Support POA&M closeout assessment and appeal resolution

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



Tips and Strategies for CMMC Compliance



Steps to CMMC Compliance

BDO'S METHODOLOGY FOR CMMC COMPLIANCE

1	SCOPE	<ol style="list-style-type: none">1. Determine contract governance and CUI discovery2. Mapping FCI and CUI in architecture, Use Cases3. Define Authorization Boundaries
2	DESIGN & IMPLEMENT	<ol style="list-style-type: none">4. Define Architectures for FCI and CUI5. Scope technical challenges6. Implement technical options
3	DOCUMENT	<ol style="list-style-type: none">7. Create Policies/Procedures/Artifacts
4	ASSESS & VALIDATE	<ol style="list-style-type: none">8. Gap Assessment9. Verification & Validation (V&V)
5	CERTIFY	<ol style="list-style-type: none">10. Certification (CMMC C3PAO)
6	MAINTAIN	<ol style="list-style-type: none">11. Train, Test, Review & Update

First Stage: Scoping

TIPS & STRATEGIES FOR CMMC COMPLIANCE

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?

Second Stage: Design & Implement

TIPS & STRATEGIES FOR CMMC COMPLIANCE

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 options
6. Secure areas of facility where CUI is processed
7. Train PMs and users how to access CUI and how to safeguard it

Third Stage: Document

TIPS & STRATEGIES FOR CMMC COMPLIANCE

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

1. **Policies & Procedures** for:
 - ▶ NIST 800-171 Non-Federal Organization (NFO) Controls
 - ▶ NIST 800-171/CMMC Level 1 controls (affects FCI)
 - ▶ 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.

Fourth Stage: Assess & Validate

TIPS & STRATEGIES FOR CMMC COMPLIANCE

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).

CASK-chat

Personnel and Role-Based Training

Expand specific training to those who handle CUI - or even the personnel that oversee CUI projects.

- ▶ Contracts Managers
- ▶ Project Managers
- ▶ Program Managers
- ▶ HR
- ▶ Facility Security
- ▶ Privileged Users

- ▶ Know how to define security training across different organizational roles.
- ▶ Everyone who handles CUI or oversees personnel that will handle CUI need to be trained.



Compliance is NOT JUST an “IT Issue”

Other stakeholders need to be involved outside of the IT department so that everyone “owns” the program.

- ▶ Company C-Suite
- ▶ Human Resources
- ▶ Facilities Security Officers/Managers
- ▶ Technical Roles & Engineers/Scientists
- ▶ Project Managers & Managers



The success of your assessment depends on the involvement of ALL stakeholders. Your IT staff are not the only stakeholders in your compliance programs!

Separation of Duties

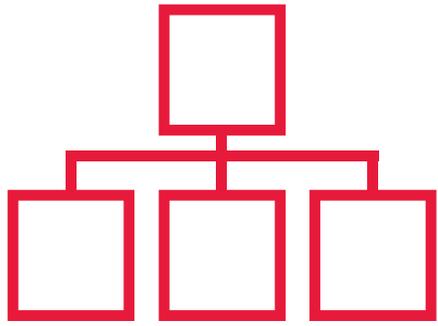
WHAT DOES THIS MEAN FOR YOUR ORGANIZATION?

When you have a lean staff, how do you employ separation of duties? One person cannot perform all duties in the organization.

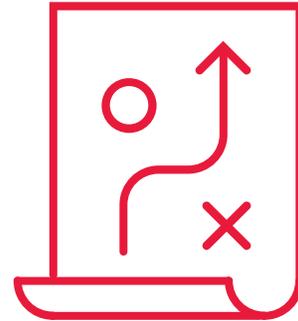
- ▶ Clearly outline Roles & Responsibilities - make sure there is at least one other person to perform a duty so there is not a single point of failure
- ▶ Do you have one person that approves accounts AND enters into the system? Make it two people.
- ▶ Does your Systems Administrator also have privileges to modify/delete audit logs? Create an Audit Administrator.
- ▶ Share responsibilities with your external providers (MSP/MSSP)

- ▶ The principle of separation of duties involves assigning different tasks of a process to more than one individual such that no one employee can solely initiate, record, authorize, and reconcile a transaction without the intervention of another.
- ▶ It is the principle that no user should be given enough privileges to misuse the system on their own.

Can We Talk about Stakeholder Buy-in?



Successful CMMC Assessments start with Stakeholder knowledge and involvement of the organization's construction and implementation of the CMMC program.



The stakeholders decide where and how you dedicate your cyber and security resources. That means they have a direct impact on how you manage cybersecurity risks.



It is critical for Stakeholder to know not only the RISK but also the COST for non-compliance.

Readiness Review is Critical

A readiness review is conducted to verify that the OSC is ready to proceed with the assessment.

- ▶ Analyze Assessment Requirements
 - Determine Assessment approach
 - Verify scope and framing
- ▶ Evaluating Evidence Non-Duplication
- ▶ Evidence Readiness
- ▶ Assessment Team Readiness
- ▶ Identify Resources and Schedule
- ▶ Identify and Manage Assessment Risks
- ▶ Overall Assessment Concerns Conducting the Assessment
- ▶ Assessment Approval



CMMC Certification

What You Need to Know Before Contracting
with an Authorized 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 NOVEMBER 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, OOU, SBU, LES, and DoD Technical Data (CTI/UCTI)
- ▶ Export Controlled Data (ITAR/EAR)

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

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?



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 area of focus 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 experience 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 knowledge 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

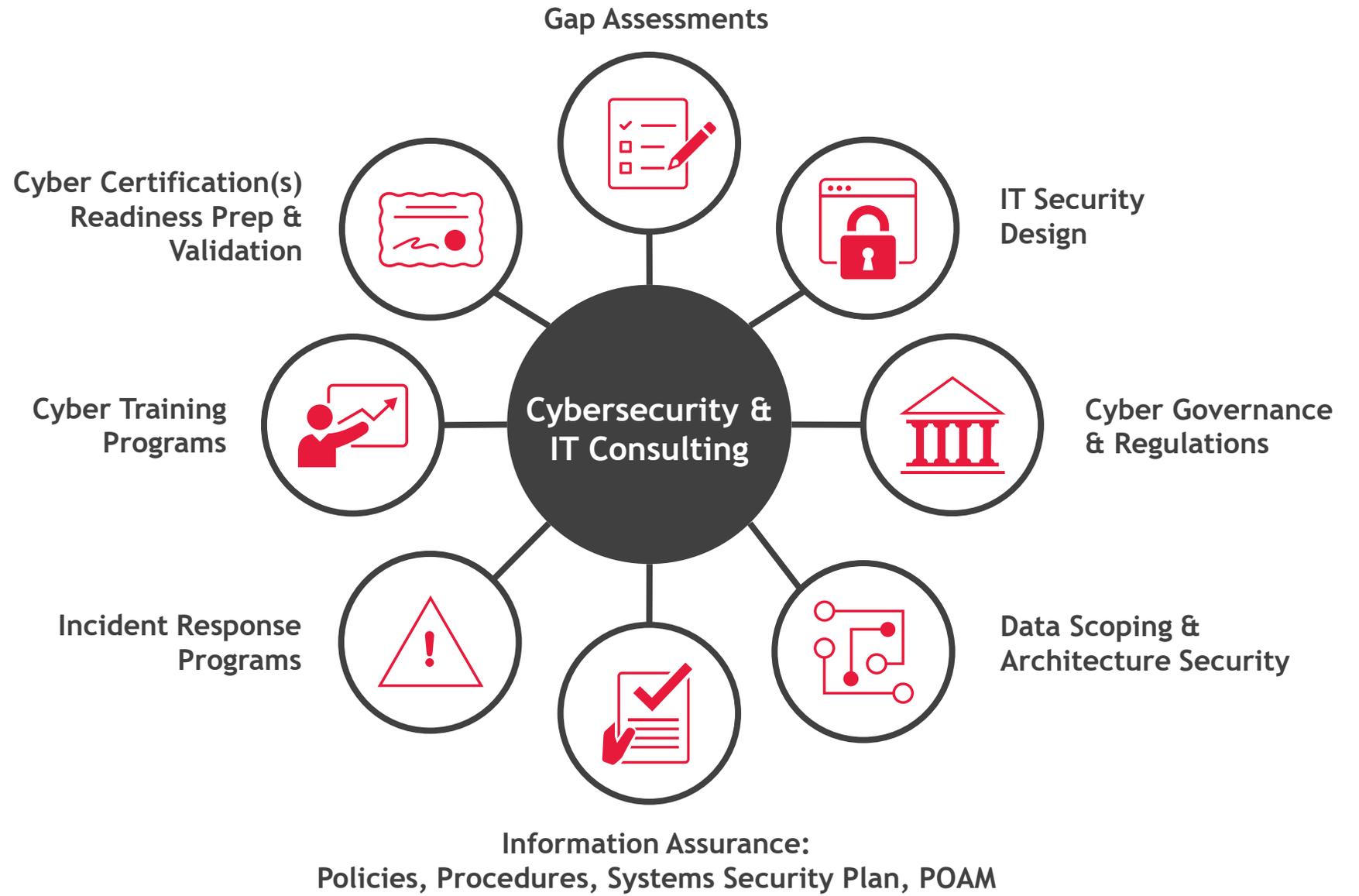
- ▶ Cyber-AB: Certified CMMC Assessor (CCA)
- ▶ Cyber AB: Provisional Assessor (PA)
- ▶ Certified CMMC Professional
- ▶ CISSP
- ▶ CNSS Risk Analyst
- ▶ CNSS System Certifier
- ▶ DoD Licenses: Marine Corps Validator
- ▶ AXELOS - Information Technology Infrastructure Library (ITIL)
- ▶ AXELOS - Resilia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

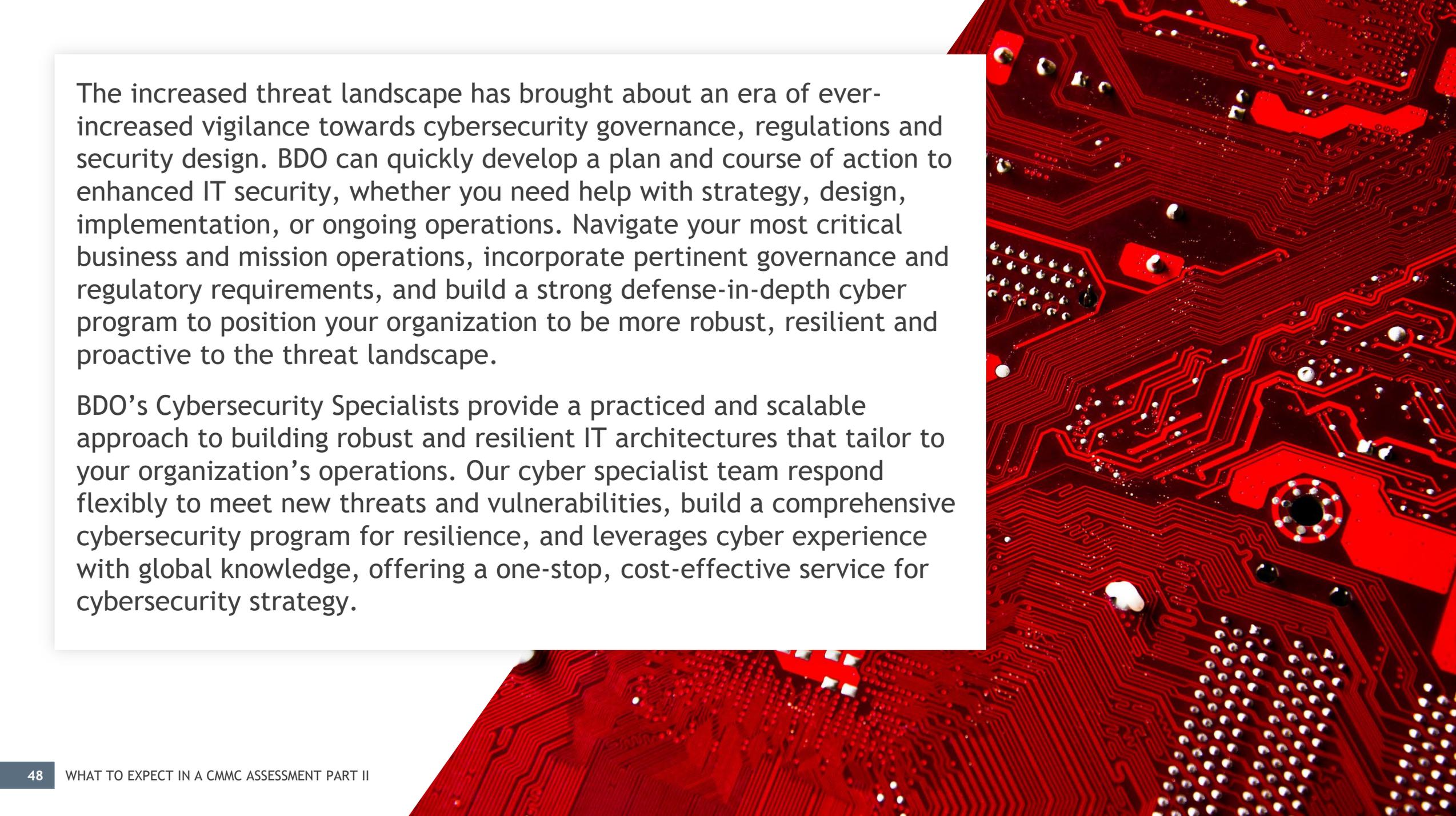
EDUCATION

- ▶ B.A. Psychology & Sociology,
Shepherd College

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.

CREDENTIALLED 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

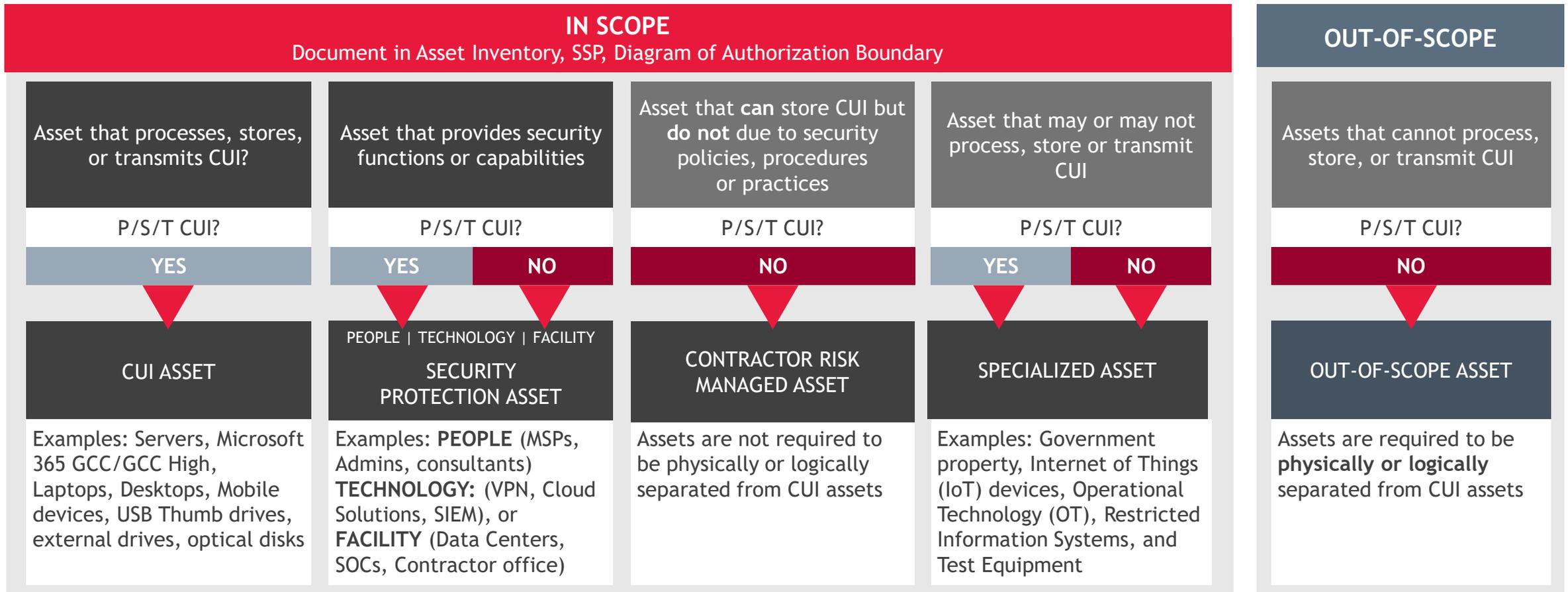
- ▶ Practiced security architecture strategies with market-leading IT platforms and services
- ▶ Flexible to incorporation of existing technologies within the environment
- ▶ Analysis of regulations and governance to meet use-case scenarios
- ▶ Cloud-based design strategies for flexible deployments to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

FOCUSED DESIGN STRATEGIES FOR BUSINESS AND MISSION

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

Extra Slides

Scoping the Environment for CUI Assets



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

Source: [Understanding Compliance Between Commercial, Government and DoD Offerings - March 2022 Update - Microsoft Community Hub](#)



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

Material discussed is meant to provide general information and should not be acted on without professional advice tailored to your needs.

WHAT IS
© 2023 BDO USA, LLP. All rights reserved.

BDO[®]