GOVERNMENT CONTRACTING
WEBCAST SERIES

Updates to the CMMC Proposed Rule

AND THE NEW DOD FEDRAMP EQUIVALENCY MEMO

FEBRUARY 21, 2024

BDO

With You Today

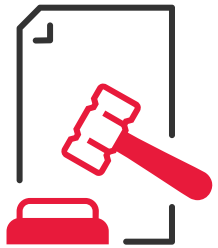
CHRISTINA REYNOLDS
CMMC Registered Practitioner (RP),
CEH, CHFI, CNDA
Industry Specialty Services Director

256-733-1115
creynolds@bdo.com

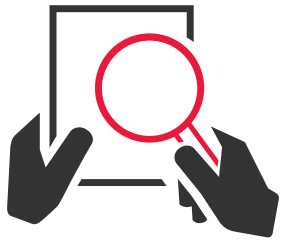
ALEJANDRO LABOY
Industry Specialty Services
Senior Manager

703-770-1055
alaboy@bdo.com

Learning Objectives

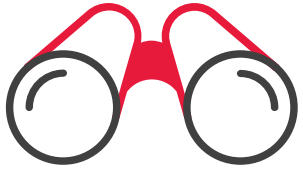


Review the key characteristics of the new CMMC proposed rule and the potential impacts to government contractors



Demonstrate approaches for recovering allowable costs related to CMMC and DFARS 7012 for Defense Contractors

Recognize strategies for building a CMMC enclave that allows large businesses to spread cost between parent and subsidiaries



Define key strategies and takeaways for small businesses

Agenda

Why Get CMMC Certified & CMMC/DFARS 7012 Timeline

CMMC Rulemaking

Scoping the CMMC Environment

FedRAMP Equivalency Memo

FCI and CUI Data Types

CMMC Cost Recovery Strategies

Questions & Answers

GOVERNMENT CONTRACTING WEBCAST SERIES

Why Get CMMC Certified & CMMC/DFARS 7012 Timeline

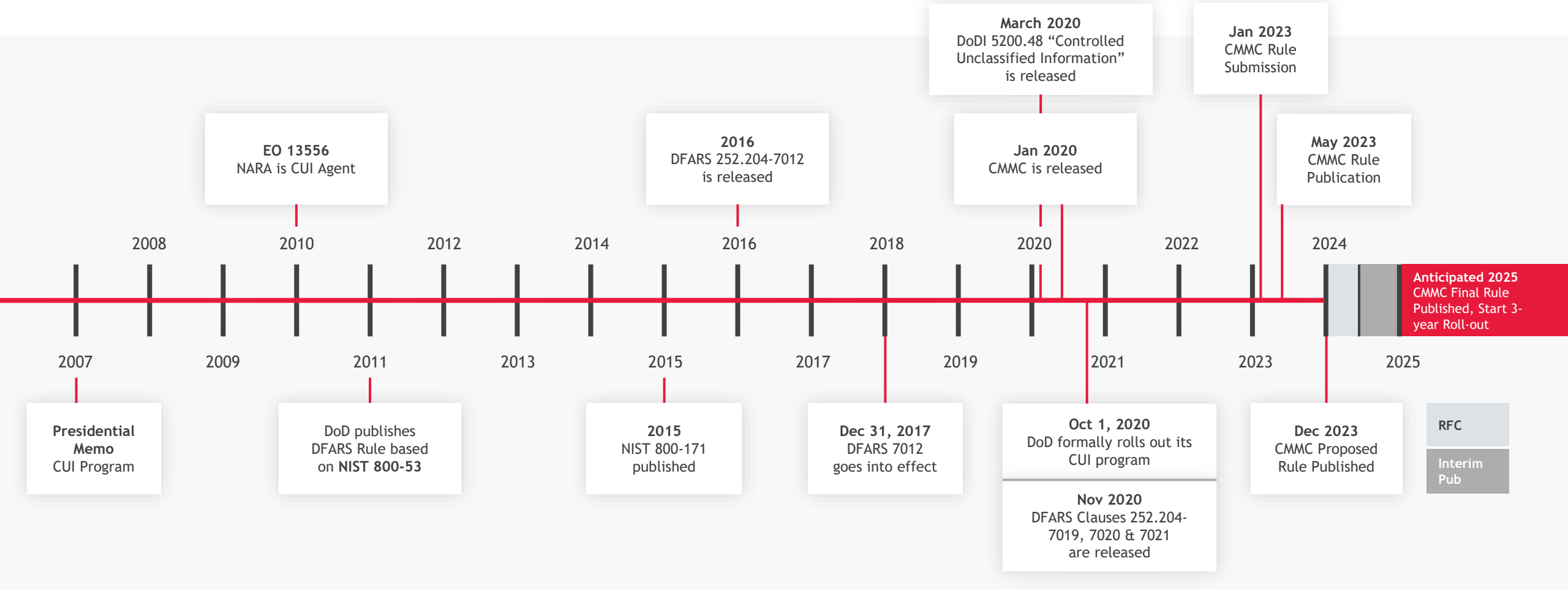
BDO

Why Get CMMC Certified?

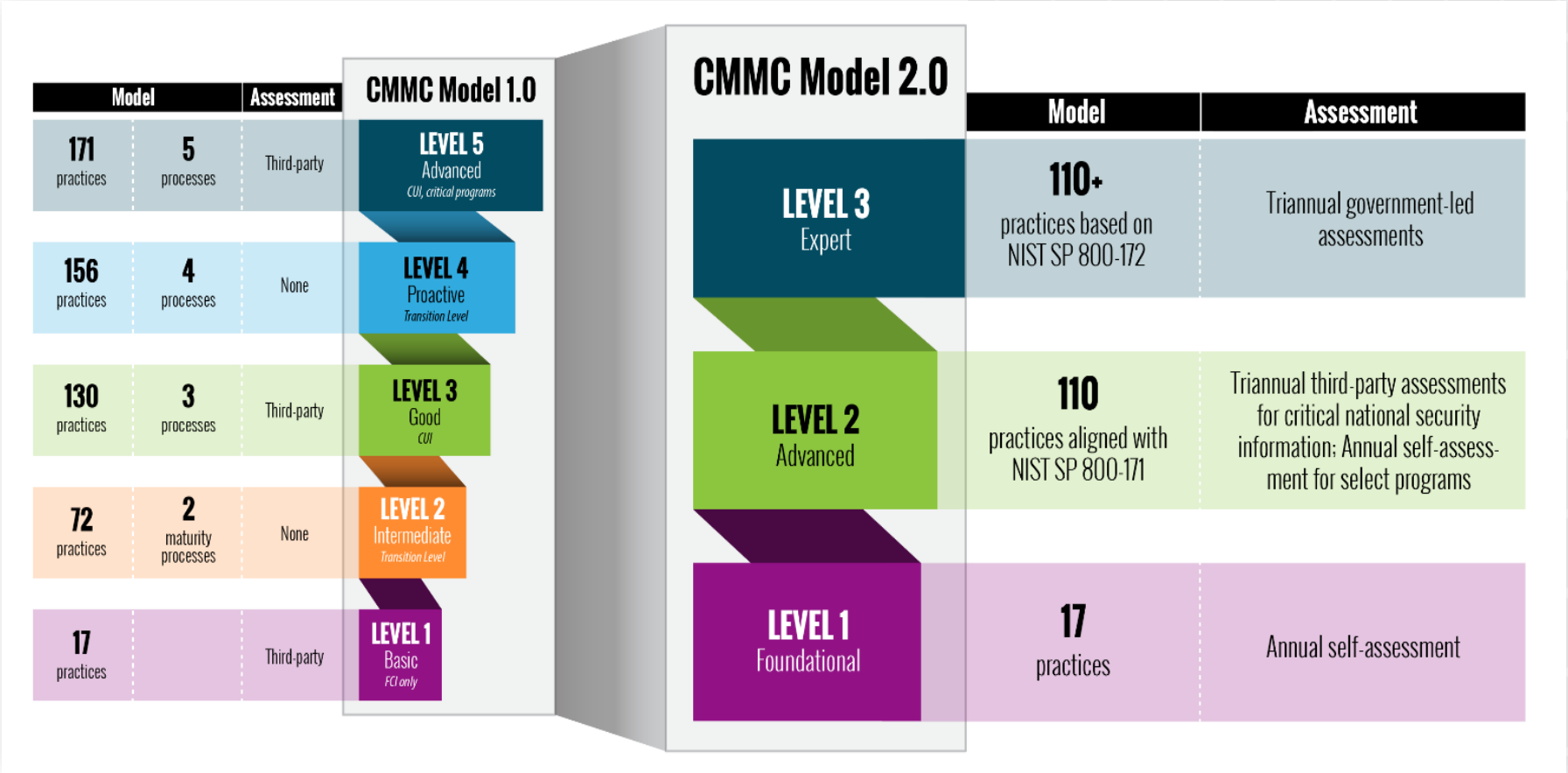
- **If you have DFARS 7012:** If you currently hold DFARS 252.204-7012 in your contracts, you will likely have a requirement for CMMC certification at Level 2 starting by 6 months after final rule is reached
- **If you currently possess CUI:** If you store, process or transmit Controlled Unclassified Information (CUI), you are already obligated to DFARS 7012 (explicitly or implicitly)
- **CMMC Mandate:** CMMC will be a mandate using the DFARS 252.204-7021 clause to place this into contracts

- **Differentiator for Government Prime Contracts:** Expect CMMC to start to be put into contracts as mandate within 6 months after CMMC Final Rule. The determination of your CMMC Certification will determine award factor
- **Teaming differentiator:** Prime will send questionnaires to determine DFARS 7012 and will add CMMC to these questionnaires as soon as Final Rule is achieved. If you don't have a certification, you may not be invited to team with the prime

DFARS 252.204-7012 and CMMC Timeline



CMMC 2.0 Processes



Source: [CMMC Model (defense.gov)]

Key Changes for CMMC 2.0

With the implementation of the Cybersecurity Maturity Model Certification (CMMC) 2.0 program, the Department is introducing several key changes that build on and refine the original program requirements. These are:

Streamlined Model

- **Focused on the most critical requirements**: Streamlines the model from 5 to 3 compliance levels
- **Aligned with widely accepted standards**: Uses National Institute of Standards and Technology (NIST) cybersecurity standards

Reliable Assessments

- **Reduced assessment costs**: Allows all companies at Level 1, and a subset of companies at Level 2, to demonstrate compliance through self-assessments
- **Higher accountability**: Increases oversight of professional and ethical standards of third-party assessors

Flexible Implementation

- **Spirit of collaboration**: Allows companies, under certain limited circumstances, to make Plans of Action & Milestones (POA&Ms) to achieve certification
- **Added flexibility and speed**: Allows the Government to waive inclusion of CMMC requirements under certain limited circumstances

Source: dodcio.defense.gov/CMMC/about/

GOVERNMENT CONTRACTING WEBCAST SERIES

CMMC Rulemaking

Information You Should Know Regarding the CMMC 2.0 Proposed Rule

BDO

CMMC Proposed Rule Published

DECEMBER 26, 2023

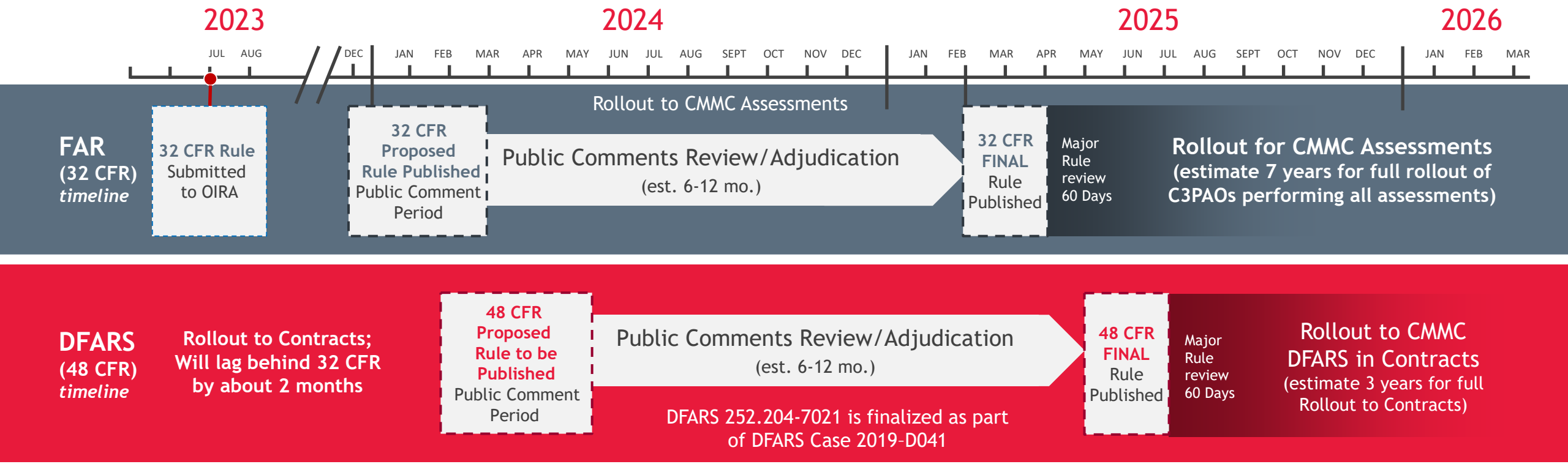
- On December 26, 2023, the Department of Defense published for comment a proposed rule for the Cybersecurity Maturity Model Certification (CMMC) 2.0 program at www.regulations.gov/docket/DOD-2023-OS-0063
- Concurrent for comment with this proposed rule, DoD is also requesting comment on eight CMMC guidance documents, which can be accessed at www.regulations.gov/docket/DOD-2023-OS-0096, and several new information collections, which are available at www.regulations.gov/docket/DOD-2023-OS-0097
- The proposed rule indicates that the DoD anticipates **139,201 companies will be subject to Level 1 Self-Assessment while bifurcated on Level 2 - 4,000 will self-attest and 76,598 will be C3PAO certification.**

The 60-day comment period, initiated on December 26th, allows stakeholders to shape the CMMC program.

Closing on February 26, 2024, this period precedes a meticulous review and response process by the DoD, which is expected to span 12-18 months.

The Final Rule is anticipated in late 2024 or early 2025. The DoD has made recent statements that it would like to publish "before the election".

FAR and DFARS CMMC Rulemaking Timelines



"The Department intends to pursue rulemaking both in Part 32 of the Code of Federal Regulations (C.F.R.) as well as in the Defense Federal Acquisition Regulation Supplement (DFARS) in Part 48 of the C.F.R. Both rules will have a public comment period. Stakeholder input is critical to meeting the objectives of the CMMC program, and the Department will actively seek opportunities to engage stakeholders as it drives towards full implementation."

Source: dodcio.defense.gov/CMMC/about/

Phased Roll-out

3-Year Rollout

CMMC Regulation into New Contracts

- DoD plans to roll-out CMMC in phases to **new** contracts to occur over 3 years.
- *"The DoD is implementing a phased implementation for the CMMC Program and intends to introduce CMMC requirements in solicitations over a three-year period **to provide appropriate ramp-up time**."* federalregister.gov/d/2023-27280/p-390

7-Year Rollout

CMMC CMMC Level 2 Certification to all DIB Contractors

- Since the requirements will only go in new contracts, it is projected to take 7 years in total as the DoD estimates around 80,000 companies will need a CMMC Level 2 assessment.
- The DoD claims the 7-year roll-out helps with the current lack of C3PAOs and the lengthy process for the assessors to become certified.
- *"DoD is planning for a phased roll-out of each assessment level across 7 years with the entity numbers reaching a maximum by Year 4 as shown in the tables."* federalregister.gov/d/2023-27280/p-417

CMMC Phased Implementation

Phase 1:
Self-Assessments

CMMC Level 1 & Level 2 Self-Assessments required as a **condition of award** for new contracts and option years

DoD Optional: CMMC Level 2

CMMC Level 2 **Certifications** may be added for applicable contracts as **condition of award** for some early contracts/option years

0-6 Months

Phase 2:
CMMC Level 2 Certifications

CMMC Level 2 Certification Assessment requirements are applied to new contracts/option years

DoD Optional: CMMC Level 3

DoD may also include CMMC Level 3 Certification Assessment requirements as it deems necessary for applicable solicitations and contracts.

6-18 Months

Phase 3:
CMMC Level 3 Certifications

DoD will insert CMMC Level 3 Certification Assessment requirements for all applicable DoD solicitations and contracts as a condition of contract award.

DoD Optional: Delay Requirements

DoD may choose to delay inclusion of CMMC requirements as appropriate.

18-30 Months

Phase 4:
Full Roll-out to All

Includes all CMMC Program requirements in all DoD solicitations and contracts, including option periods.

30+ Months

CMMC Proposed Rule

BIG TAKEAWAYS

Phased deployment (4 Phases)

Requires third-party assessments on all contracts at the beginning of Phase 2, **which is six months after the final rule goes into effect, and self-assessments on all new contracts as soon as the final rule becomes effective.**

Bifurcated Assessment Requirements for Level 2

Level 2 is a split level (some assessments are self-assessments and some are third-party assessments), the DoD anticipates that a CMMC Third-Party Assessment Organization (C3PAO) will conduct most Level 2 assessments (4,000 entities completing a self-assessment versus 76,598 entities receiving a third-party assessment).

DoD will leverage the False Claims Act (FCA)

Third-party Level 2 assessments require a company executive to file an affirmation with the DoD upon the conclusion of the third-party assessment and every year after that. Level 1 assessments require a company executive to certify the assessment to the DoD. The DoD will undoubtedly contend that these certifications are significant.

3-Year Certification

The duration of third-party assessments is three years, though this might be shortened if the contractor makes significant changes to the system that has been evaluated/granted certification. When attempting to arrange an assessment with a C3PAO, organizations awaiting a third-party assessment may find themselves in competition with those receiving a second evaluation.

GWACS Contracts

The federal supply schedule and other Federal Agency contracts, like NASA's Solutions for Enterprise-Wide Procurement (SEWP), may already be implementing CMMC certification requirements prior to CMMC Final Rule. Use Q&A during RFI/RFP to ask for it to be removed – more appropriate on Task Order-level.

CMMC Proposed Rule

BIG TAKEAWAYS

External Service Providers (ESPs like MSP and MSSPs)

The Proposed Rule integrates an understanding that one of the biggest growing concerns is the role that managed service providers (MSPs) and Managed Security Service Providers (MSSPs) now play in CMMC environments for organizations of all sizes. There is some discussion about requiring ESPs to meet their client's obligations for a specific CMMC level of certification – but the teeth for this lies in the Contractor to impose on their provider.

JVSA Certifications

Currently only 100% perfect Joint Surveillance Voluntary Assessments (JSVA) results, free of open POAMs, offer a direct transfer to CMMC Level 2 certification. DIBCAC has said that it will work to follow up with the C3PAOs and OSCs to assess if open POAM items are closed out within the 180-day timeframe, with the intent to get all who are diligently closing out controls to get their certification.

Allowable Open POA&M Items

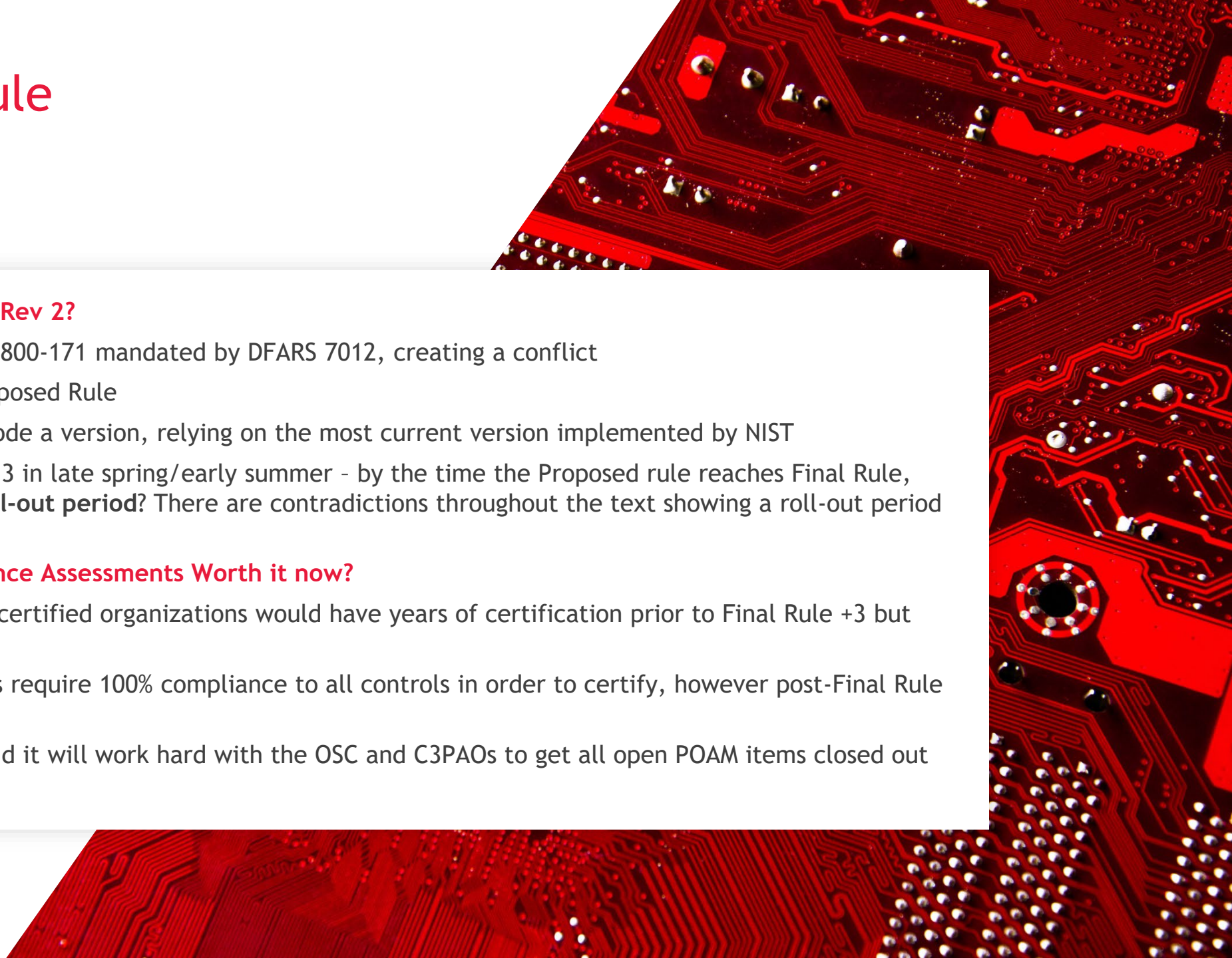
While current certifications require 100% compliance, Once the Final Rule is published, a Plan of Action and Milestone (POA&M) is allowed. While a minimum of 80% is allowed to achieve a certification, the highest-weighted security controls (think the -5 and -3 controls) must be addressed first within 180 days of the initial assessment.

Operations Technology (OT)

OT equipment are to be "documented but not assessed" against other CMMC requirements. Assessors are to "review the SSP" but are not to "assess against other CMMC requirements". While this may be a breath of relief, for manufacturers, it does not really address mis-fit of CMMC to OT environments.

CMMC Proposed Rule

POTENTIAL ISSUES



- **Hard-Coding NIST 800-171 at Rev 2?**
  - DoD has hard-coded NIST SP 800-171 mandated by DFARS 7012, creating a conflict
  - Rev 2 all throughout the Proposed Rule
  - DFARS 7012 does not hard-code a version, relying on the most current version implemented by NIST
  - NIST will be introducing Rev 3 in late spring/early summer – by the time the Proposed rule reaches Final Rule, NIST 800-171 Rev will be **Roll-out period**? There are contradictions throughout the text showing a roll-out period of 3 years versus 7 years
- **Are Joint Voluntary Surveillance Assessments Worth it now?**
  - Initially promised that JVSA certified organizations would have years of certification prior to Final Rule +3 but that is no longer the case
  - Additionally, currently JVSAs require 100% compliance to all controls in order to certify, however post-Final Rule it will be lower-80% to pass
  - Note that the DIBCAC has said it will work hard with the OSC and C3PAOs to get all open POAM items closed out within the 180 days

Scoping the CMMC Environment

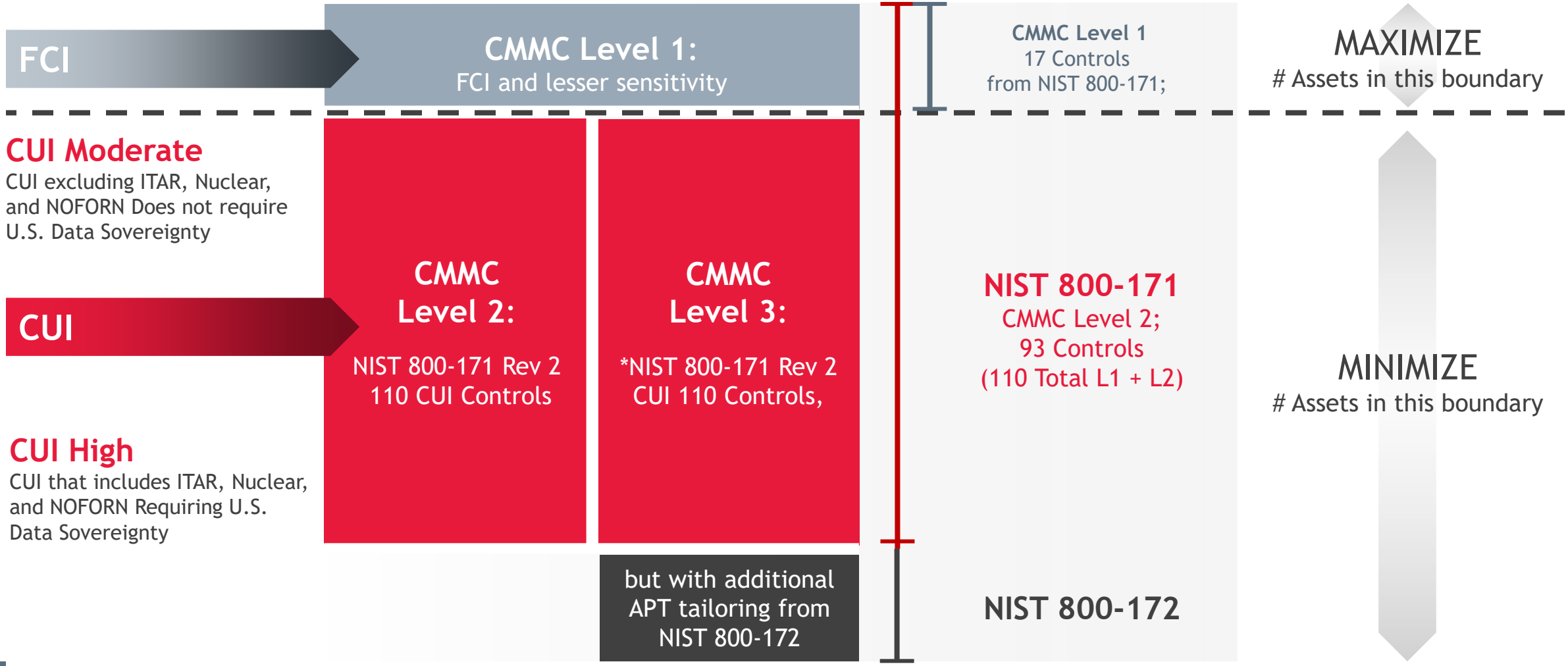
IT Environment Scoping Should be Strategic

- The most crucial component of building a CMMC program is the environment scoping. A properly pre-planned scope can reduce overall cost of both implementation and ongoing management and will additionally streamline the CMMC certification assessment process.
- **CMMC Level 1** can be Federal Contract Information (FCI) and below.
  Out of scope: CUI and above Sensitivity.
  - **Seek to maximize this footprint by eliminating CUI from this boundary and any assets that don't need to process CUI.**
- **CMMC Levels 2 & 3** environments include anything that can process, transmit or store CUI, or those assets that are interconnected to CUI systems, simply because they **may** receive CUI). This includes security protection assets such as routers and firewalls and potentially can also cover Internet of Things and Operations Technology. Please refer to the scoping diagram.
  - Organizations must completely meet Level 2 standards to add on Level 3 controls (NIST 800-172) for **Advanced Persistent Threat protection** as **enhanced controls** onto the NIST 800-171 baseline.

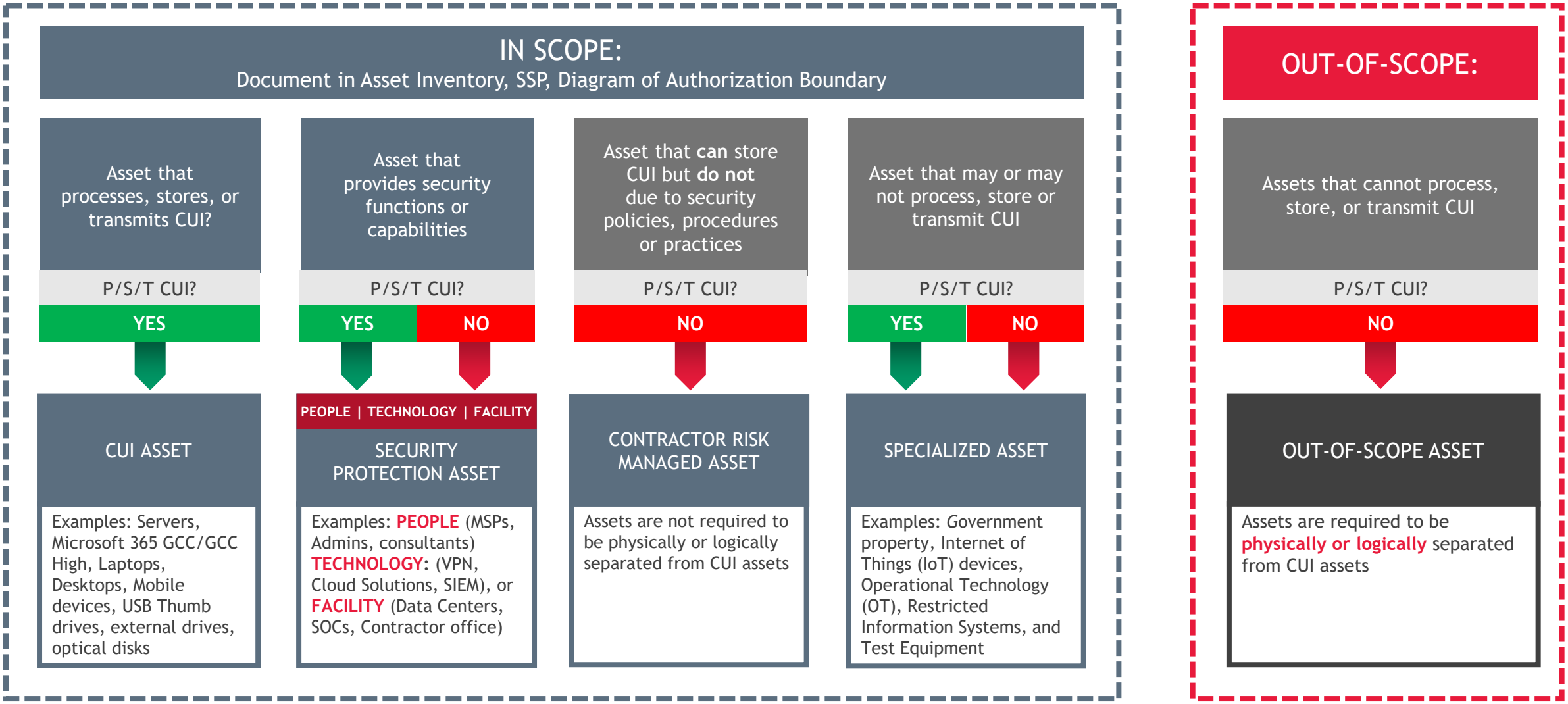
Seek to minimize this boundary by only including JUST THOSE ASSETS that require CUI to be processed through, transmitted, or stored upon them.

This effort of **minimizing assets storing CUI** and segregating both physically and logically these assets while **maximizing a lower data threshold** for your environment will minimize both business risk for mishandling of data and will minimize costs for CMMC certification and ongoing management.

Strategic Scoping is Key to CMMC Success!

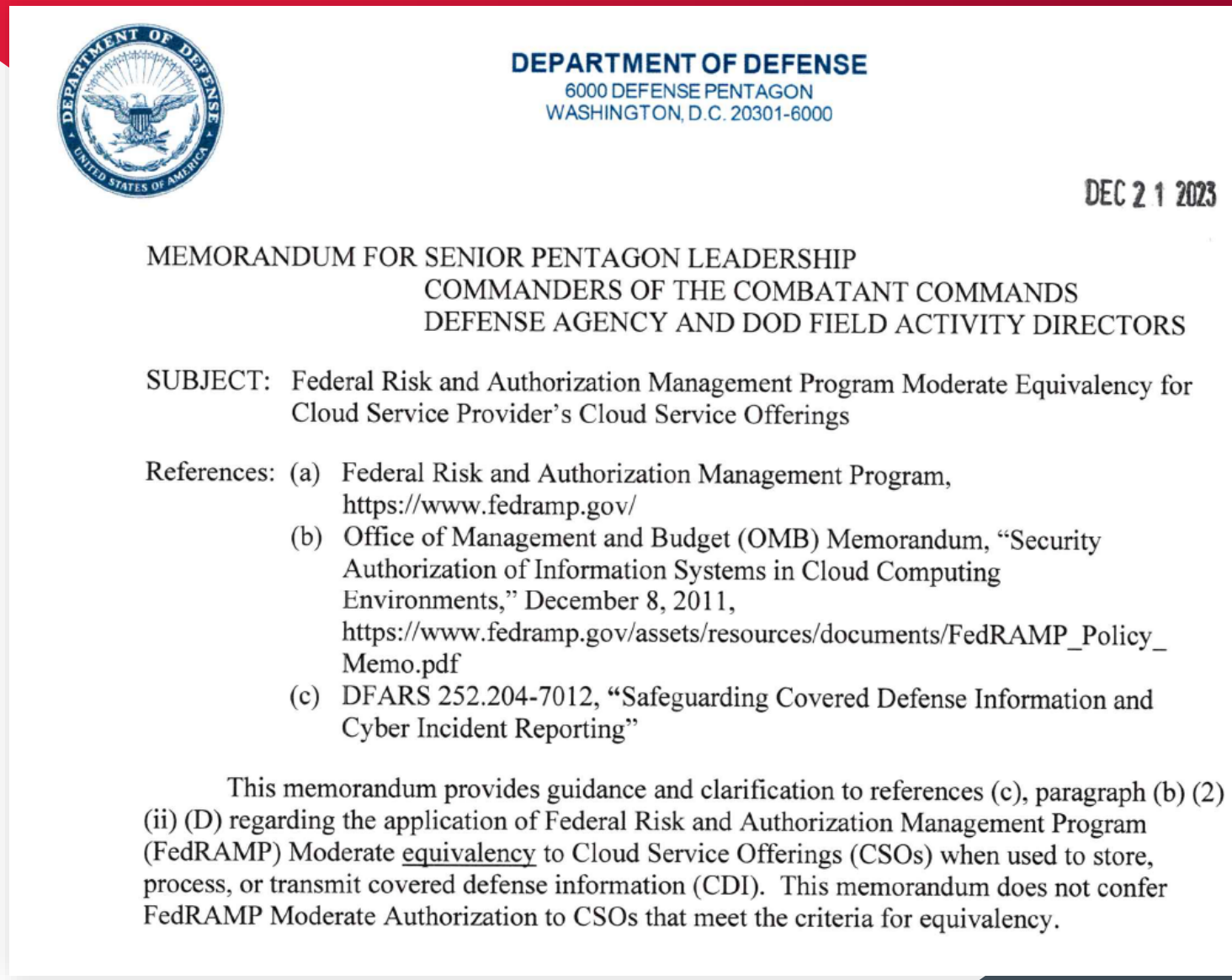


CMMC 2.0: Scoping the Environment for CUI Assets



FedRAMP Equivalency Memo

DoD FedRAMP Equivalency Memo



DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

DEC 21 2023

MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP
COMMANDERS OF THE COMBATANT COMMANDS
DEFENSE AGENCY AND DOD FIELD ACTIVITY DIRECTORS

SUBJECT: Federal Risk and Authorization Management Program Moderate Equivalency for Cloud Service Provider's Cloud Service Offerings

References: (a) Federal Risk and Authorization Management Program, https://www.fedramp.gov/
(b) Office of Management and Budget (OMB) Memorandum, "Security Authorization of Information Systems in Cloud Computing Environments," December 8, 2011, https://www.fedramp.gov/assets/resources/documents/FedRAMP_Policy_Memo.pdf
(c) DFARS 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting"

This memorandum provides guidance and clarification to references (c), paragraph (b) (2) (ii) (D) regarding the application of Federal Risk and Authorization Management Program (FedRAMP) Moderate equivalency to Cloud Service Offerings (CSOs) when used to store, process, or transmit covered defense information (CDI). This memorandum does not confer FedRAMP Moderate Authorization to CSOs that meet the criteria for equivalency.

FedRAMP Equivalency Memo Takeaways

- Does not apply to those CSOs who are already FedRAMP Authorized/have an ATO
- Applies to CSOs that that do not yet have a FedRAMP ATO but know their environment stores CDI/CUI on behalf of their commercial DIB end-clients.
- Perhaps put too much instruction in one memo – there's instruction for the DIB Contractor to vet their CSO solutions, but also instruction for the CSP to create a "FedRAMP equivalent" package - this should perhaps be 2 separate memos
- References DFARS 7012 – so onus is on DIB Contractors to
  - Understand what Cloud Service Offerings (CSOs) they store CDI/CUI in and
  - Require those providers to either certify they have a FedRAMP Moderate ATO or FedRAMP Equivalency certified by a FedRAMP CPAO

What may change soon:

- Memo **will likely be rescinded** pending the new Executive Order coming out for FedRAMP
- DoD will re-word memo with cooperation from FedRAMP, then re-issue
- Change 100% compliance to a lesser %?

FedRAMP Questionnaire for Clients

SaaS/Cloud Vendor Questionnaire

Cloud Service Offering (CSO) *(product Name, Version, etc)*		Provider Company Name / Address
Product Name		
Version		

Package ID Name if on FedRAMP Marketplace:

Cloud Service Offering type:	CSO Hosted Environment Impact Level
☐ SaaS ☐ IaaS ☐ PaaS	☐ IL 2 – Accommodates DoD information that has been approved for public release (Low Confidentiality & Moderate Integrity)
Cloud Hosted Platform Provider	☐ **IL 4** – Accommodates DoD Controlled Unclassified Information (CUI)
☐ **AWS Gov Cloud**	☐ **IL 5** – Accommodates DoD CUI & National Security System (NSS)
☐ AWS Commercial Cloud	☐ **IL 6** - Accommodates DoD Classified Information up to SECRET
☐ **Microsoft Azure Gov Cloud**	**FedRAMP Moderate or High?**
☐ Microsoft Azure Commercial Cloud	☐ Moderate ☐ High
☐ **Google Public Sector Cloud**	**FedRAMP Approval by which Entity?** *(JAB, FedRAMP Board or Fed/DoD Agency)*
☐ Google Cloud	☐ JAB
☐ Other / Hosted Data Center: *Please note below*	☐ FedRAMP Board
-	☐ Specific Agency: Name of Agency

If CSO has ATO: *(please put N/A if you are not Sponsored on the FedRAMP Marketplace)*	Answer
Does this **SaaS product** have a FedRAMP ATO?	
- If yes, Does the SaaS product have Full ATO or Interim ATO?	

REMINDER

This Was Already in DFARS 7012

FedRAMP Moderate Baseline Equivalency was already "baked in"

From DFARS 252.204-7012:

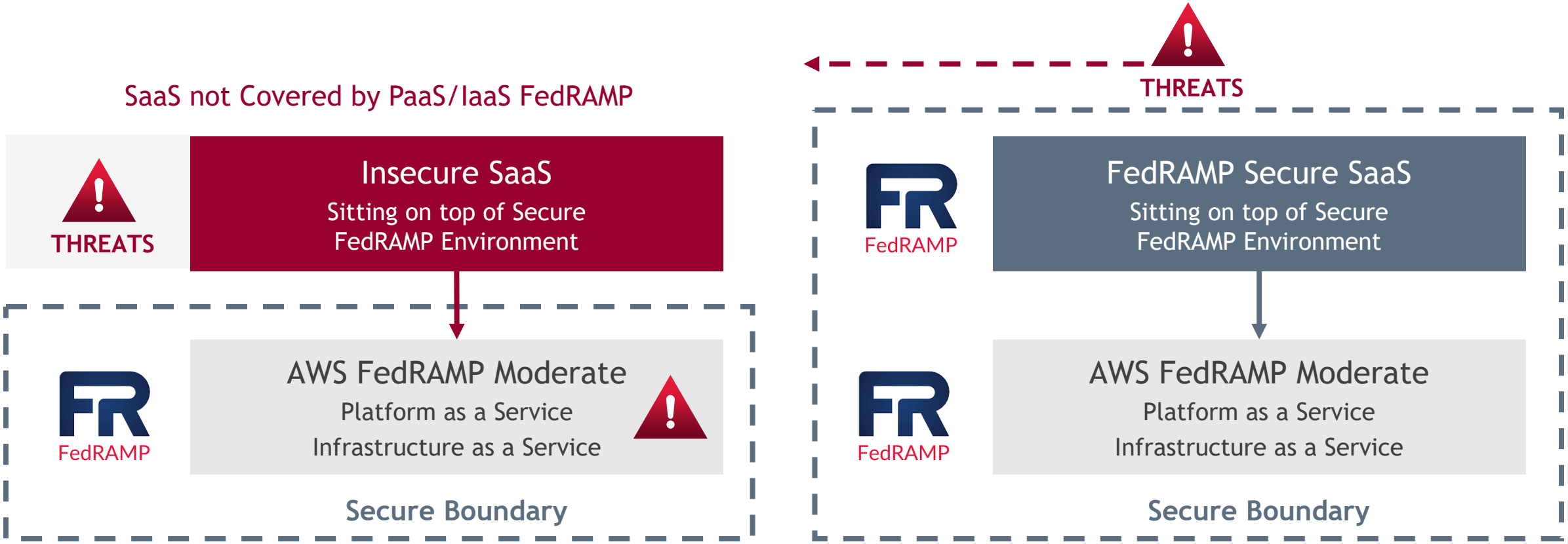
- "(D) If the Contractor intends to use an external cloud service provider to store, process, or transmit any covered defense information in performance of this contract, the Contractor shall require and ensure that the **cloud service provider meets security requirements equivalent to those established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

The FedRAMP Equivalency Memo was nothing new…

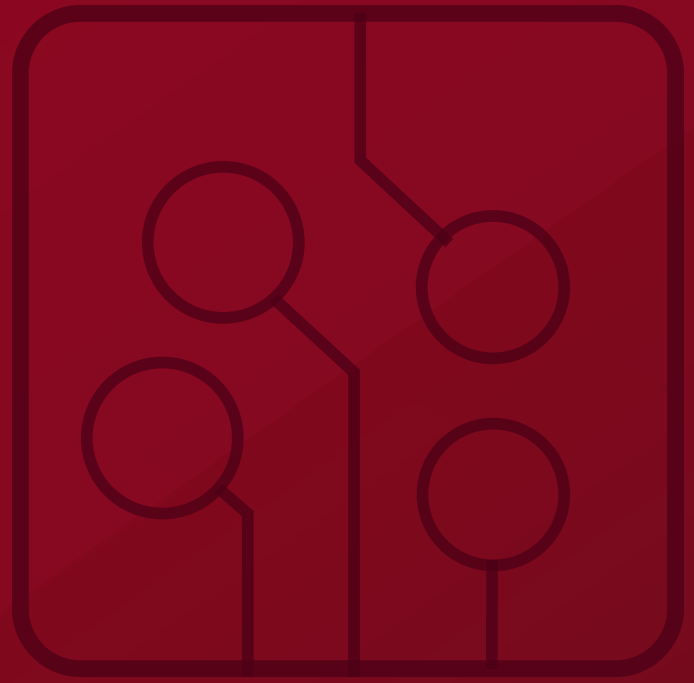
These requirements for external cloud service providers [used by the Contractor to store CDI/CUI] to be FedRAMP Moderate Equivalent have always been in your contract requirements!

Why Does a SaaS Product Need to be Compliant to NIST 800-171?

It is **NOT ENOUGH** for the SaaS to claim that it is FedRAMP Authorized because it is sitting on a FedRAMP Cloud Hosted Platform; the SaaS must also be FedRAMP to transmit or store Govt Data.



FCI and CUI Data Types



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.
EXEMPTION	▶ 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 (including services)
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

DFARS 252.204-7012

SAFEGUARDING FOR CONTROLLED UNCLASSIFIED INFORMATION (CUI)

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

Defines CUI

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.

NARA archives: Classification for CUI Categories
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

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	COTS, 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

Controlled Technical Information (CTI) 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

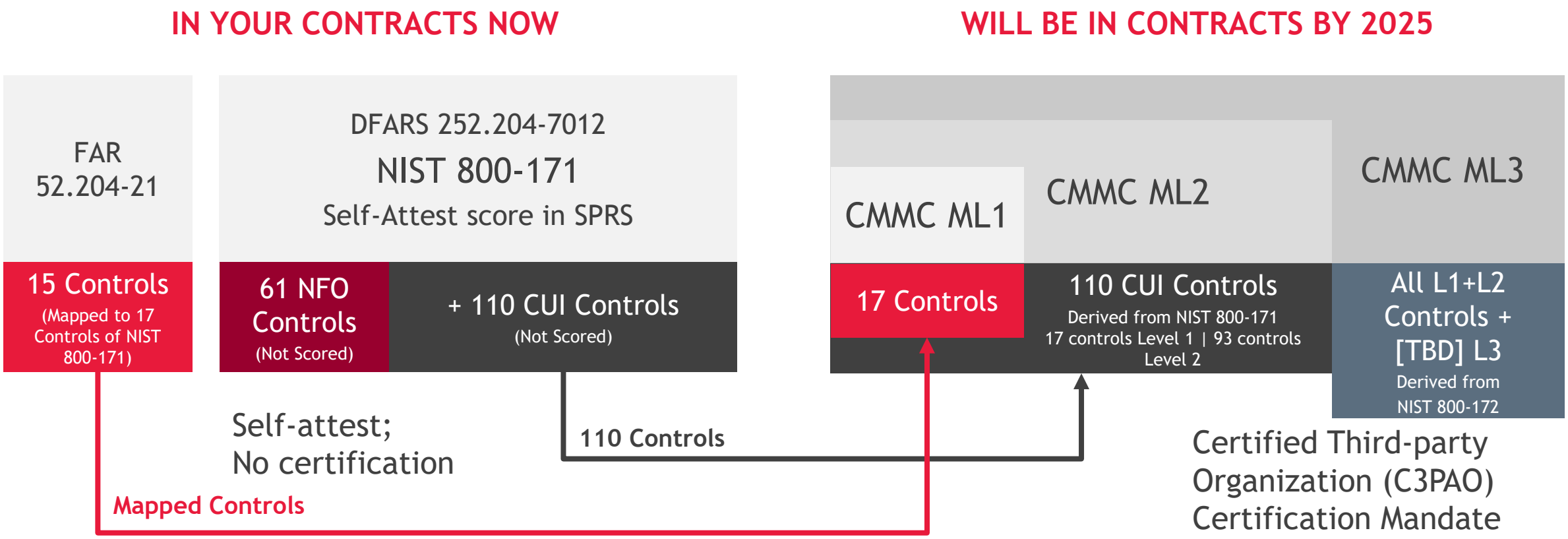
Does not include:

- Commercial products
- Commercial services

The Additional 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 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 (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

Security Controls and Inheritance Between Frameworks



GOVERNMENT CONTRACTING WEBCAST SERIES

CMMC Cost Recovery Strategies

BDO

What Are Indirect Rates?

- Indirect rates are computed factors or percentages representing the ratio of selected indirect expenses to specific elements of cost or other performance metrics.
- Specific elements of cost used for calculation commonly include direct labor, subcontracts or a combination of various manufacturing activities; other performance metrics may include direct labor hours or units of output or production.
- Typical indirect rates are computed and associated with fringe benefits, overhead and general & administrative type activities.

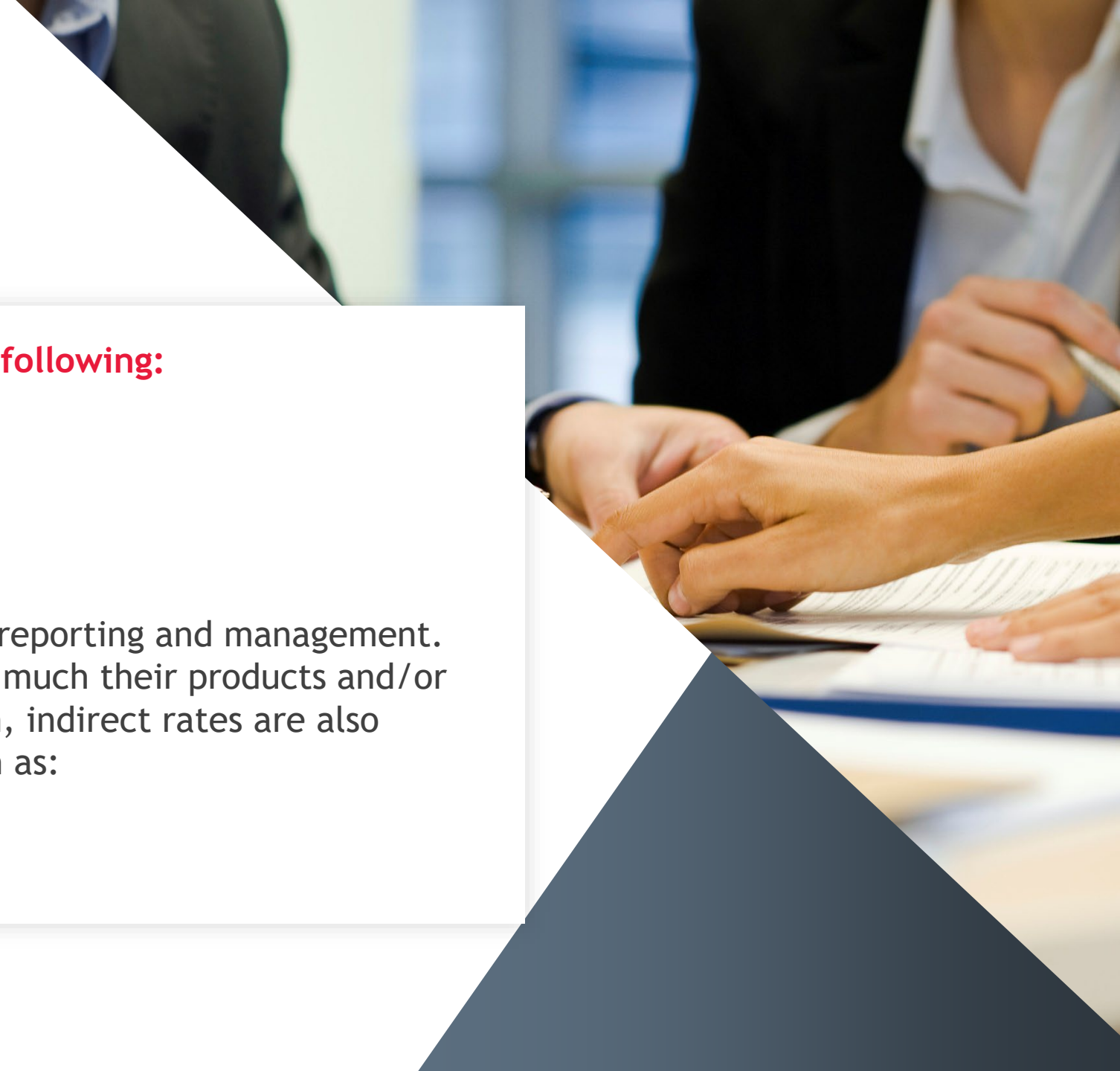
Why Are Indirect Rates Important?

Indirect rates are a critical component to fully pricing out products or services.

Indirect rates provide contractors with a mechanism to:

- Assign indirect costs to their contracts and grants
- Subsequently invoice and be reimbursed for the allowable costs it incurs on its flexibly-priced contracts.

Why Are Indirect Rates Important?



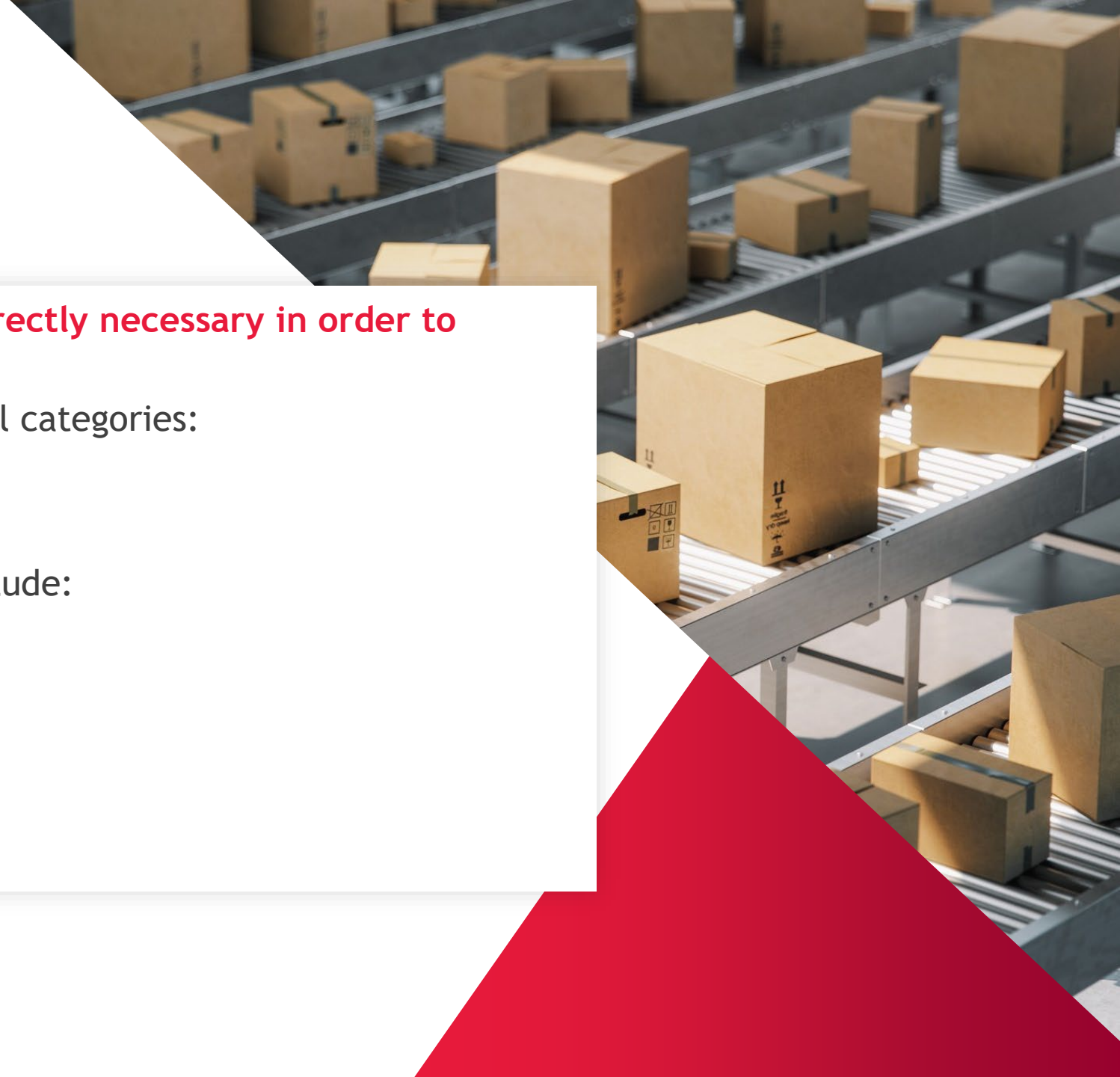
Indirect rates are used in pricing for the following:

- Proposals
- Invoices and billings
- Requests for equitable adjustment
- Termination settlement

Indirect rates are also critical for internal reporting and management. They allow contractors to understand how much their products and/or services are actually costing them. As such, indirect rates are also important for organizational purposes such as:

- Internal Management Reporting
- Budgeting and Resource Consumption

Direct Costs



Direct costs are the expenses that are directly necessary in order to produce goods or provide services.

Direct costs typically fall into three general categories:

- Direct labor (DL)
- Direct materials (DM)
- Other direct costs (ODCs); examples include:
  - Direct subcontractor costs
  - Consultant services
  - Direct travel
  - Packaging & freight
  - Cybersecurity Costs?

Indirect Costs

An indirect cost is a cost that cannot be practically or reasonably assigned directly to the production or performance of a particular product or service.

Indirect costs are not incurred for the benefit of a single objective or contract, but rather, to support the organization or business unit as whole.

Examples of indirect costs include:

- Executive management (i.e. CEO, CFO, COO, President/VP, etc.) salaries and benefits
- Employee benefits costs
- Accounting & HR department salaries and benefits
- Legal fees
- IT costs
- Facilities costs

Direct or Indirect Cost?

Would this cost have been incurred if the specific contract/final cost objective did not exist?

NO ➡ DIRECT COST

YES ➡ INDIRECT COST

Direct or Indirect Cost?

DIRECT COSTS

Expenses that directly go into producing goods or providing services

Direct labor

Direct materials

Manufacturing supplies

INDIRECT COSTS

General business expenses that keep you operating

Rent

Utilities

General office expenses

Importance of Direct & Indirect Costs

Accordingly, a contractor must have the ability to:

- Identify direct costs versus indirect costs
- Segregate direct costs from indirect costs and accumulate direct and indirect costs separately based on logical groupings
- Indirect costs are not incurred for the benefit of a single objective or contract, but rather, to support the organization or business unit as whole

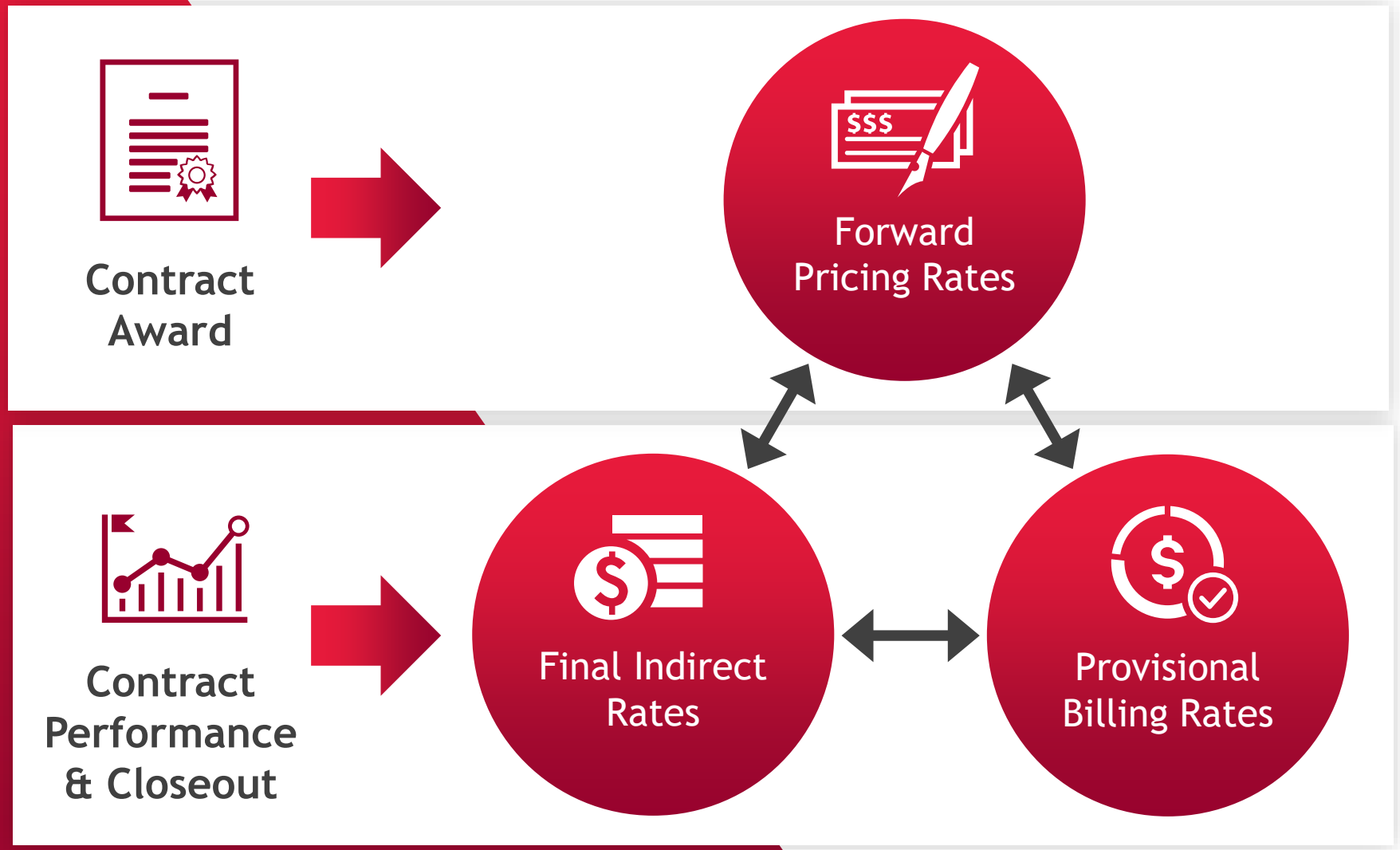
What is the significance of direct and indirect costs?

- Government allows contractors to recover their costs or a portion thereof
- Direct costs are directly identified to their respective contracts and may be recovered 1-for-1
- Allowable indirect costs are allocated to a contract using indirect rates

How does a contractor do this?

- Project/job codes (direct and indirect)
- General ledger account numbers (i.e. chart of accounts)

Indirect Rates Within the Contract Lifecycle



Indirect Rates Within the Contract Lifecycle

Forward Pricing Rates

- Best estimate of indirect cost rates at the time of submission
- Typically used to estimate pricing for future periods of Government contract work
- Usually a 3 to 5 year projection

Provisional Billing Rates

- Used for interim billing of costs
- Subject to true-up at year end
- Established by Contracting Officer or Auditor
- Revised as necessary based on mutual agreement
- Should be updated soon after year-end

Indirect Rates Within the Contract Lifecycle

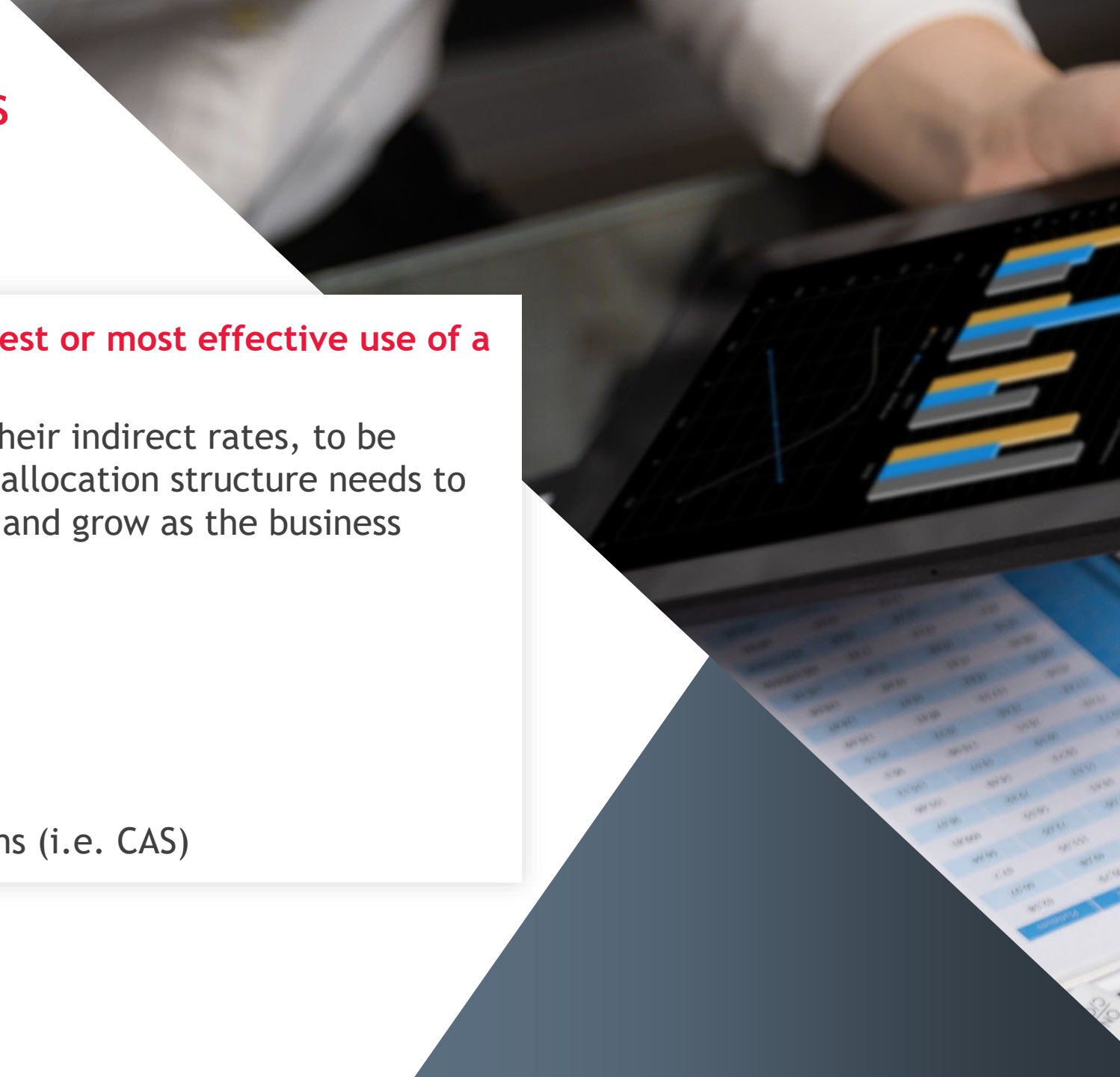
Final Indirect Rates:

- Due 6 months after year-end (Final Indirect Cost Rate Proposal)
- Final billings for completed contracts are due within 120 days after settlement of rates
- Quick-Closeout Procedures

Negotiated or audit-determined final indirect rates are used for:

- Billing updates (impact differences in provisional rates)
- Contract close-out
- Preparation of completion vouchers (due within 120 days after settlement of final indirect costs rates for contracts)
- Determination of final incentive/award fees

Indirect Rates Considerations



Optimization: The action of making the best or most effective use of a situation or resource.

Companies want their costs, in particular their indirect rates, to be competitive in the marketplace. Your cost allocation structure needs to support your business strategy, and evolve and grow as the business evolves and grows:

- New operating locations
- New programs
- New contract types (FP, CP, T&M)
- Contracts with different cost content
- Ensuring compliance with new regulations (i.e. CAS)

Indirect Rates Considerations

- **Cost is Cost:** Sometimes the key is how you package and present the rates
  - Address the perception of “high rates”
  - “Squeeze the Balloon”
  - Recover all allowable cost
- Concept of Full Absorption Costing: All your costs need to be accounted for, and all indirect costs need to be allocated and absorbed by the benefiting “final cost objectives”
- Assess your organization structure and make sure it reflects how you want to run your business, both now and in the future.
- Org structure informs the number of cost centers/departments/pools.

Indirect Rates Considerations

AGGRESSIVE APPROACH

- Maximize cost recovery on USG contracts
- Typical approach for “pure” government contractors
- Typical approach for contractors with cost-plus contracts
- Increased audit exposure and compliance requirements

CONSERVATIVE APPROACH

- Choose not to recover certain higher-risk costs
- More typical for businesses with more commercial contracting mix

Indirect Rates Considerations

Other Cost Allocation Considerations:

- Direct vs Indirect
- Service Center pools
  - Facilities
  - IT
  - Shared Services
- Home Office structures
- Intermediate Level Home Office(s)

Special Allocations

- A special allocation is a corrective allocation that makes an individual cost objective (allocation recipient) whole from use of the normal allocation methodology.
- A special allocation is what you do when your standard cost accounting practices do not result in an equitable distribution of indirect costs.
- The contractor and the Cognizant Federal Agency Official “may agree” to the use of special allocations (or may not).
- Government auditors will focus on special allocations, and Contracting Officers will expect to see a detailed Advance Agreement for their execution before you implement them

Indirect Rates Considerations

Applicable framework and US Government regulations and oversight:

- Federal Acquisition Regulations:
  - FAR Part 31 Cost Principles
- Defense Federal Acquisition Regulations Supplements
  - DFARS 252.204-7021
    - CMMC Level 1 – 3 - Indirect
    - CMMC Level 4 -5 - Direct
- Cost Accounting Standards
  - CAS 403 – Home Office Allocations
  - CAS 410 - G&A Allocation
  - CAS 418 – Direct vs. Indirect Costs
- Defense Contract Audit Agency
  - Billing updates
  - Court determinations

Best Practice

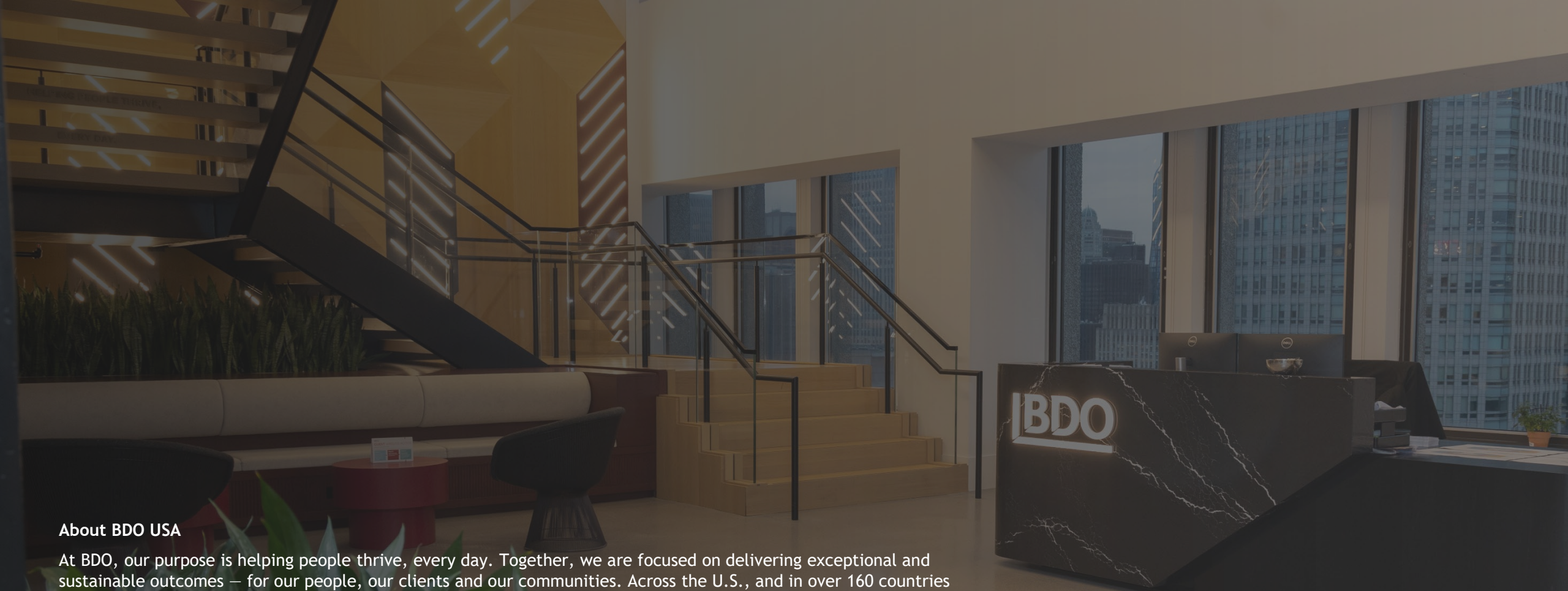
- **Understand your business**: Anticipate future contracts and plan your structure accordingly
- **Maintain good documentation** describing your rate structure and how costs are included in your pools and bases (CASB Disclosure statement)
- **Review your practices** at least annually to ensure that they are consistent with the policies established; if there have been changes, identify if they meet one of the exceptions to a cost accounting practice change
- **Know your practices** as of the date of award or CAS coverage. How were costs bid?
- If changes are contemplated, **communicate with DCAA/ACO**: Tell your story

Questions & Answers

BDO CMMC RPO Accredited Status

BDO is a CMMC Registered Practitioner Organization (RPO) and is listed in Active Status on the CMMC-AB Marketplace

cmmcab.org/marketplace/bdo-usa-llp-rpo/



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, P.C, a Virginia professional corporation, 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