GOVERNMENT CONTRACTING
WEBCAST SERIES

Handling ITAR and Export Control Data

EXCEPTIONS FOR EXISTING AGREEMENTS AND CYBERSECURITY IMPLICATIONS

MARCH 20, 2025

BDO

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.

With You Today

CHRISTINA REYNOLDS
Managing Director and CMMC CCP
Industry Specialty Services
BDO USA, P.C.

creynolds@bdo.com

ERICA BAKIES
Partner
Seyfarth Shaw LLP

ebakies@seyfarth.com

Learning Objectives

Upon completion of this session, participants will be able to:

Recognize the key components of the Cybersecurity Maturity Model Certification (CMMC) framework & data protections for CUI & ITAR

Identify relevant ITAR exception strategies that can be utilized on U.S. Government defense contracts to enable authorized foreign national contractor employees to access ITAR & Export-Controlled sensitive data

Determine strategies for scoping an organizations' environment that ensures an efficient assessment & compliances with CUI & ITAR data security requirements & U.S. Data Sovereignty

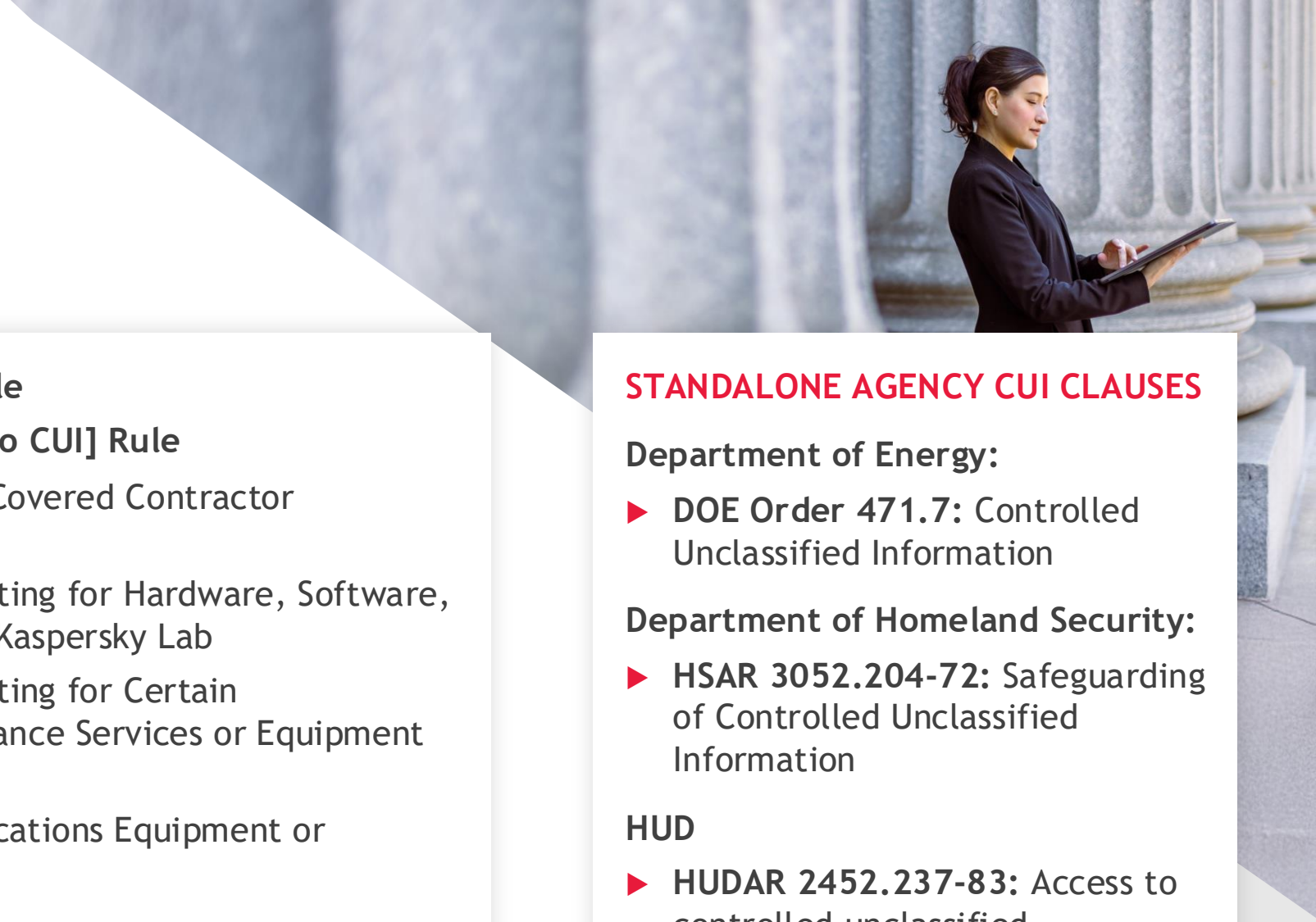
GOVERNMENT CONTRACTING WEBCAST SERIES

CUI Regulations and CMMC

BDO

Federal Acquisition Regulation (FAR)

CYBERSECURITY CLAUSES



- **FAR 52.204-XX: New Proposed CUI Rule**
- **FAR 52.204-YY: New FAR Proposed [No CUI] Rule**
- **FAR 52.204-21:** Basic Safeguarding of Covered Contractor Information Systems
- **FAR 52.204-23:** Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab
- **FAR 52.204-25:** Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment (Section 889)
- **FAR 52.204-26:** Covered Telecommunications Equipment or Services—Representation
- **FAR 52.204-27:** TikTok Prohibition
- **FAR 52.239-1:** Privacy or Security Safeguards

STANDALONE AGENCY CUI CLAUSES

Department of Energy:

- **DOE Order 471.7:** Controlled Unclassified Information

Department of Homeland Security:

- **HSAR 3052.204-72:** Safeguarding of Controlled Unclassified Information

HUD

- **HUDAR 2452.237-83:** Access to controlled unclassified information (CUI)

Department of Defense (DoD)

CYBERSECURITY CLAUSES

- **DFARS 252.204-7008:** Compliance with Safeguarding Covered Defense Information Controls
- **DFARS 252.204-7009:** Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information
- **DFARS 252.204-7012:** Safeguarding Covered Defense Information and Cyber Incident Reporting
- **DFARS 252.204-7018:** Prohibition on the Acquisition of Covered Defense Telecommunications Equipment or Services
- **DFARS 252.204-7019:** Notice of NIST SP 800-171 DoD Assessment Requirements
- **DFARS 252.204-7020:** NIST SP 800-171 DoD Assessment Requirements
- **DFARS 252.204-7021:** Cybersecurity Maturity Model Certification (CMMC) Requirements *New in rulemaking 48 CFR
- **DFARS 252.204-7024:** Notice on the Use of the Supplier Performance Risk System
- **DFARS 252.225-7048:** Export-Controlled Items
  - **Export Administration Regulations (EAR)** - Controls the export of dual-use and commercial items
  - **International Traffic in Arms Regulations (ITAR)** - Controls the export and import of defense-related articles and services
- **DFARS 252.239-7010:** Cloud Computing Services
- **DFARS 252.239-7016:** Telecommunications Security Equipment, Devices, Techniques, and Services

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
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 Flowdown 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)

1 **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

2 **EXEMPTION**

Commercial products and commercial services

3 **FLOW DOWN**

Mandatory flow down to subcontractors for which subcontract performance **will involve covered defense information**, including subcontracts for commercial products or commercial services.

4 **MARKING**

Basic or Specified CUI markings (see NARA CUI List)

EXAMPLE CUI CATEGORY:

Controlled Technical Information with Military or Space Applications:

- 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

Click to Read Article Source ▶

Cybersecurity Maturity Model Certification (CMMC)

FINAL RULEMAKING

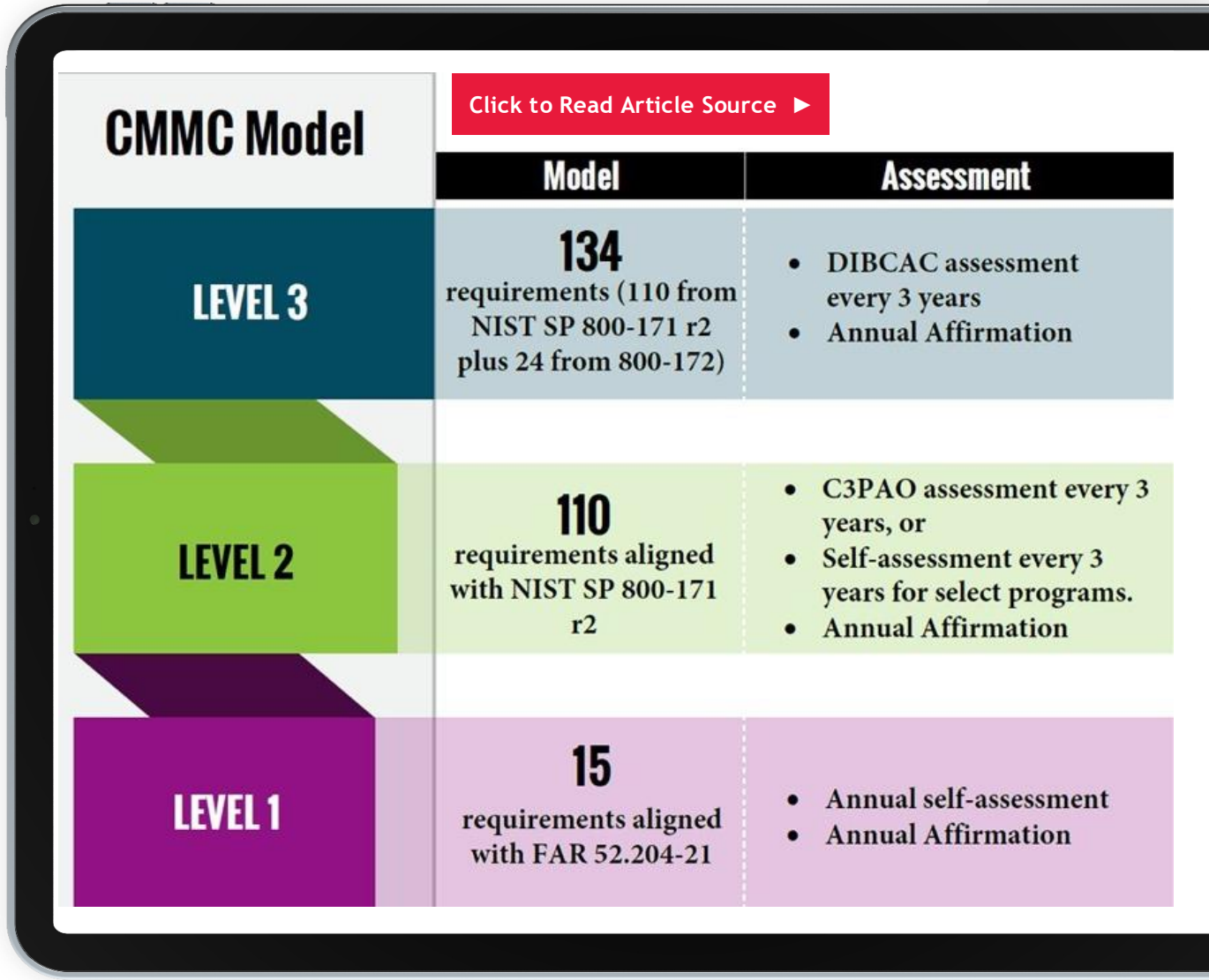
- The 32 CFR CMMC Final Rule was published in the Federal Register and approved by congress as of **December 16, 2024**.
- The **48 CFR will be finalized in 2025** to finalize DFARS 252.204-7021, the clause mandating CMMC certification in Gov contracts.
- Mandates a **CMMC-certified C3PAO third-party certification** of contractors' systems and practices to ensure they meet the required CMMC levels.
- The proposed rule offers **a 4-phase rollout** after Final Rule is released.

- Proposes **3 levels** of cybersecurity maturity, enabling organizations of varying capabilities to be appropriately assessed and certified.
- All DIB contractors **MUST be Level 1 at a minimum** and will be required to be Level 2 if receiving or storing Controlled Unclassified Information (CUI).
- Expected to impact over 300,000 entities within the DIB, with almost 80,000 required to be CMMC Level 2 either via self-attest (about 4,000) or **CMMC Certification (about 76,000)** within 12-24 months after Final Rule.

CMMC 2.0: Levels of Certification

WHY IS THIS IMPORTANT?

- Must be CMMC L2 and above if you handle ITAR!



GOVERNMENT CONTRACTING WEBCAST SERIES

What is ITAR?

BDO

ITAR

ITAR stands for **International Traffic in Arms Regulations**. It's a set of U.S. government regulations that control the export and temporary import of defense-related items and services. The purpose of the ITAR is to protect U.S. national security and further U.S. foreign policy interests.

How ITAR works

- The U.S. Department of State's Directorate of Defense Trade Controls (DDTC) administers the ITAR
- ITAR regulates “defense articles,” which are items with military properties, and related technical data
- ITAR also regulates “defense services,” which includes the furnishing of certain assistance related to defense articles, technical data, and training to foreign persons
- “Defense articles” and “defense services” are those identified on the ITAR’s U.S. Munitions List (“USML”)
- The USML has 21 Categories, ranging from firearms to missiles to explosives to ground vehicles to aircraft to military electronics

The Department of State is responsible for the export and temporary import of defense articles and defense services governed by **22 U.S.C. 2778 of the Arms Export Control Act (AECA)** and **Executive Order 13637.**

Penalties for ITAR violations

- Penalties for ITAR violations include civil fines of up to $1,271,078 per violation and/or debarment
- Criminal fines of up to $1 million and/or 20 years imprisonment per violation, per violation

Click to Read Article Source ▶

Export-Controlled Items

"Export Controlled" may indicate CUI will be on the Contract: DFARS 252.225-7048 "Export-Controlled Items"

DFARS 252.225-7048 reiterates a Contractor's obligation to comply with all applicable laws and regulations regarding export-controlled items, including, but not limited to, the registration with the DDTC when required by the ITAR. The Contractor shall consult with the Department of State regarding any questions relating to compliance with the ITAR and shall consult with the Department of Commerce regarding any questions relating to compliance with the EAR. Any federal contract information with this clause should be safeguarded on FedNet.

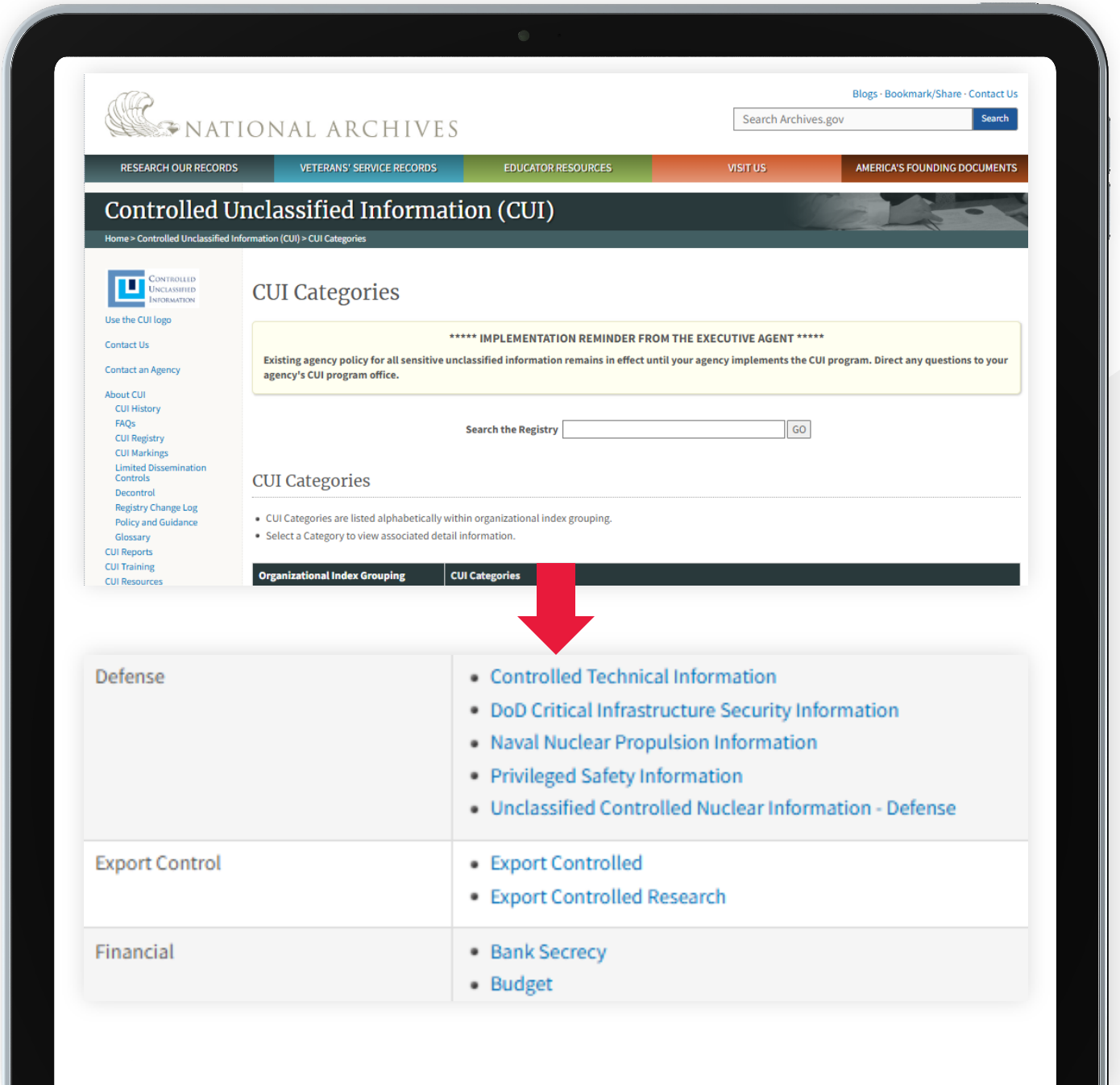
The applicable regulations and laws may include:

- The Export Administration Act of 1979, as amended (50 U.S.C. App. 2401, et seq.)
- The Arms Export Control Act (22 U.S.C. 2751, et seq.)
- The International Emergency Economic Powers Act (50 U.S.C. 1701, et seq.)
- The Export Administration Regulations (15 CFR Parts 730-774)
- The International Traffic in Arms Regulations (22 CFR Parts 120-130)
- Executive Order 13222, as extended
- Contractors are also required to flow down this clause to their subcontractors

NARA CUI Categories

EXPORT CONTROLLED INFORMATION **IS** CUI

Click to Read Article Source ►



CUI Category

EXPORT CONTROLLED 1/2

CUI Category: Export Controlled

Banner Marking for Specified Authorities: CUI//SP-EXPT

Banner Marking for Basic Authorities: CUI

Category Description:	Unclassified information concerning certain items, commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives. To include dual use items; items identified in export administration regulations, international traffic in arms regulations (ITAR) and the munitions list; license applications; and sensitive nuclear technology information.
Category Marking:	EXPT
Alternative Banner Marking for Basic Authorities:	CUI//EXPT
Banner Format and Marking Notes:	Banner Format: CUI//Category Marking//Limited Dissemination Control

CUI Category

EXPORT CONTROLLED 2/2

Safeguarding and/or Dissemination Authority	Basic or Specified	Banner Marking	Sanctions
50 USC 4614(c)	Basic	CUI	
13 USC 301(g)	Basic	CUI	
15 CFR 736, Supplement No. 2	Specified	CUI//SP-EXPT	
42 USC 2077(a)	Specified	CUI//SP-EXPT	
42 USC 2156	Basic	CUI	
42 USC 2168(a)	Basic	CUI	42 USC 2168(b) 42 USC 2168(c)
15 CFR 718.3	Specified	CUI//SP-EXPT	
22 CFR 124.9(a)(5)	Basic	CUI	22 CFR 127.3
22 CFR 120.21	Specified	CUI//SP-EXPT	
50 USC 4605(l)(5)	Basic	CUI	
15 CFR 748.1(c)	Specified	CUI//SP-EXPT	
15 CFR 760.5(c)	Specified	CUI//SP-EXPT	
10 USC 130(a)	Basic	CUI	
32 CFR 250.4(a)	Basic	CUI	
32 CFR 250.9	Specified	CUI//SP-EXPT	

ITAR vs. CUI Restrictions

ITAR (International Traffic in Arms Regulations) and CUI (Controlled Unclassified Information) are both classifications for sensitive data that require strict access controls and protection, but the ITAR specifically focuses on defense articles and related technical data and is considered a CATEGORY OF CUI.

KEY POINTS ABOUT ITAR RESTRICTIONS:

Access Limitations:

- Only U.S. **persons** can access ITAR controlled data without additional authorization.

Data Storage:

- ITAR data must be stored on secure servers located **within the United States**.

Strict Documentation:

- Detailed records must be kept regarding the transfer and access of ITAR data.

KEY POINTS ABOUT CUI RESTRICTIONS:

Different levels:

- CUI can be further categorized into "CUI Basic" and "CUI Specified," with varying levels of protection requirements.
- Doesn’t necessarily have NOFORN unless marked as such (limited dissemination)

NIST SP 800-171 compliance:

- CUI requires adherence to NIST SP 800-171 cybersecurity standards for data protection.

Click to Read Article Source ►

U.S. Citizen/Persons Requirements

- U.S. Person
  - Any
- Foreign Person/Foreign National
  - Any

KEY:

X = Not Required

 = Exceeds Requirement but not specified

✓ = Required/specified

Minimum Safeguarding Requirements for U.S. Personnel

Marking	U.S. Citizen	U.S. Persons	U.S. Nationals
Federal Contract Information	X	X	X
CUI (Moderate)	X	X	X
CUI ITAR		✓	X
CUI Nuclear Data	✓	X	✓

New FAR Proposed Rule: DoD, GSA and NASA

POSTED 1/15/2025

Click to Read Article Source ▶

© BDO

FAR CUI Proposed Rule

REGULATORY BACKGROUND AND RULE OVERVIEW

In November 2010, the Obama Administration issued Executive Order 13556, which appointed NARA to implement uniform CUI program requirements for all federal contracts.

The CUI program was codified in the Code of Federal Regulations at 32 C.F.R. Part 2002 six years later, but in the years that followed, only the Department of Defense formalized contractual requirements directing contractors to safeguard CUI in accordance with standards set forth at 32 C.F.R. Part 2002. See, e.g., DFARS 252.204-7012.

However, with the release of the proposed FAR CUI Rule, contractors and subcontractors across all federal agencies will soon be subject to more stringent CUI cybersecurity, training, and incident reporting requirements.

The FAR CUI Rule proposes a litany of changes to the FAR intended to standardize CUI handling, but the rule can be broken down into three basic building blocks:

- **Standard Form (SF) XXX, Controlled Unclassified Information Requirements**
- **FAR Clause 52.204-XX, Controlled Unclassified Information**
- **FAR Clause 52.204-YY, Identifying and Reporting Information That Is Potentially Controlled Unclassified Information**

The proposed FAR CUI Rule would apply to all solicitations and contracts except for solicitations and contracts solely for the acquisition of commercially available off-the-shelf (COTS) items.

GOVERNMENT CONTRACTING WEBCAST SERIES

Scoping the IT Environment for ITAR

BDO

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.

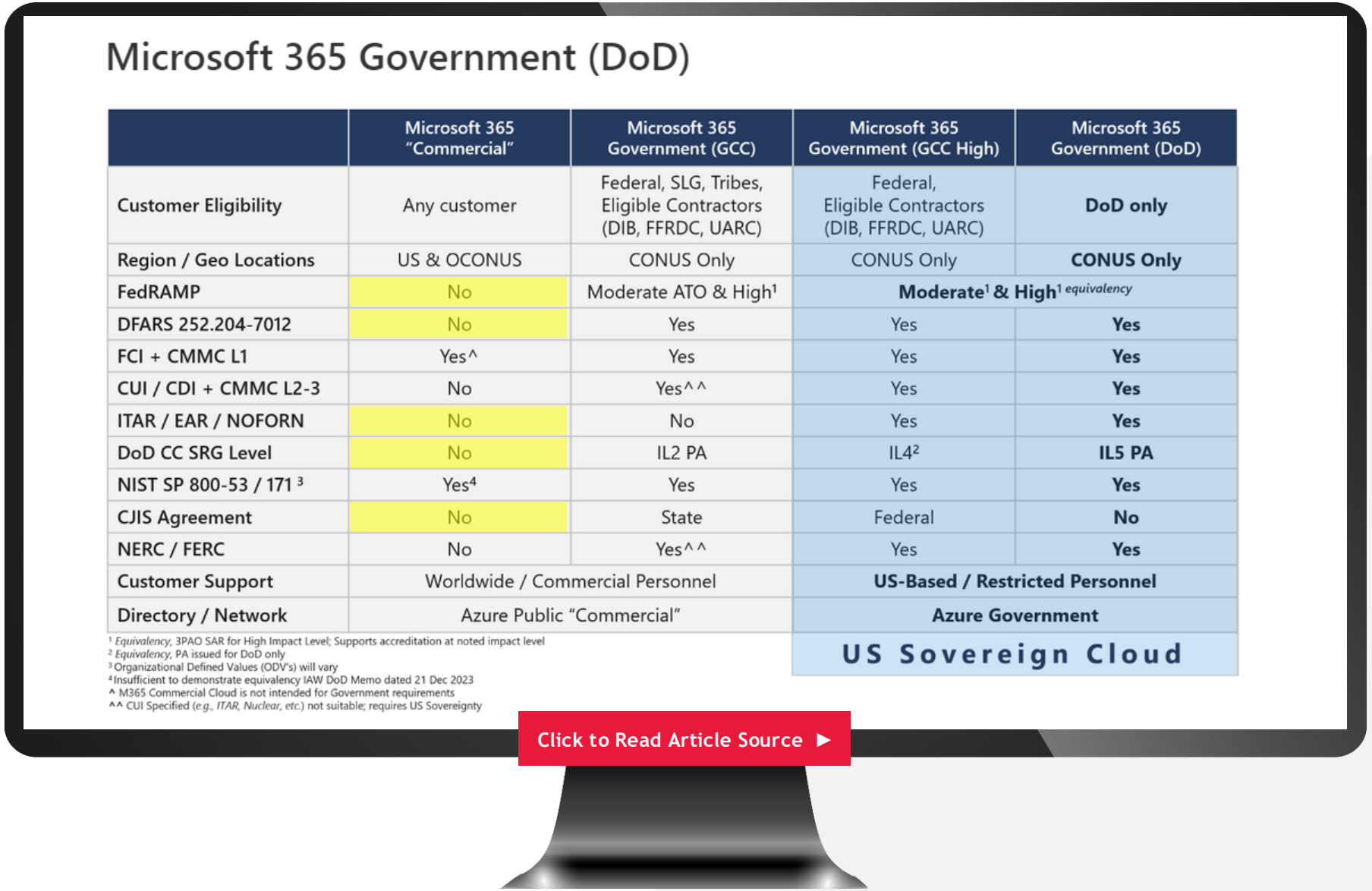
This effort of **minimizing assets storing CUI** and segregating both physically and logically these assets while **maximizing a lower data threshold** for your environment will minimize both business risk for mishandling of data, and will minimize costs for CMMC certification and ongoing management.

Scoping Is Critical!

The most crucial component of building a CMMC program is the environment scoping. While a poorly defined scope might cause an organization to incur more cost and management of compliance across multiple solutions or a wider scope, a properly pre-planned scope can reduce cost and streamline the certification process and management.

- **CMMC Level 1: FCI and Lesser Sensitivity**
  Level 1 can be Federal Contract Information (FCI) and below. Out of scope: CUI and above Sensitivity.
- **CMMC Level 2: CUI Moderate, or CUI High (Includes ITAR/U.S. Data Sovereignty)**
  CUI Moderate-scoped environment would be Microsoft GCC hosted on Azure Commercial and excludes ITAR or Nuclear data. A CUI High-Scoped environment would be Microsoft GCC High hosted on Azure Gov Cloud and contains all CUI and ITAR/Nuclear.
  - Level 2 environments, including anything that can process, transmit or store CUI simply because it's interconnected to CUI systems. 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.
- **CMMC Level 3: CUI Moderate/High but with Additional APT Tailoring**
  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.

Microsoft 365 Government (DoD)



	Microsoft 365 "Commercial"	Microsoft 365 Government (GCC)	Microsoft 365 Government (GCC High)	Microsoft 365 Government (DoD)
Customer Eligibility	Any customer	Federal, SLG, Tribes, Eligible Contractors (DIB, FFRDC, UARC)	Federal, Eligible Contractors (DIB, FFRDC, UARC)	**DoD only**
Region / Geo Locations	US & OCONUS	CONUS Only	CONUS Only	**CONUS Only**
FedRAMP	No	Moderate ATO & High[1]	**Moderate[1] & High[1]** *equivalency*	
DFARS 252.204-7012	No	Yes	Yes	**Yes**
FCI + CMMC L1	Yes^	Yes	Yes	**Yes**
CUI / CDI + CMMC L2-3	No	Yes^^	Yes	**Yes**
ITAR / EAR / NOFORN	No	No	Yes	**Yes**
DoD CC SRG Level	No	IL2 PA	IL4[2]	**IL5 PA**
NIST SP 800-53 / 171 [3]	Yes[4]	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 Public "Commercial"		**Azure Government**	
			US Sovereign Cloud	

[1] *Equivalency*, 3PAO SAR for High Impact Level; Supports accreditation at noted impact level
[2] *Equivalency*, PA issued for DoD only
[3] Organizational Defined Values (ODV's) will vary
[4] Insufficient to demonstrate equivalency IAW DoD Memo dated 21 Dec 2023
^ M365 Commercial Cloud is not intended for Government requirements
^^ CUI Specified (*e.g., ITAR, Nuclear, etc.*) not suitable; requires US Sovereignty

The High Cost of Export Control Violations

Export Control Violations

BOEING

When: February 2024

Allegation: Boeing disclosed almost 200 export violations, including its unauthorized export of technical data to China.

Outcome: Boeing reached a settlement with the U.S. State Department.

Dollar Impact: $51 Million civil penalty. $24 million of the penalty would be suspended to allow Boeing to strengthen its compliance program. Boeing will also have to engage an "external special compliance officer" for at least two years and agree to at least two external audits of its compliance program.

RTX

When: August 2024

Allegation: RTX violated the AECA and ITAR more than 750 times in relation primarily to the unlicensed export of defense articles and technical data to China, Iran, Lebanon, and Russia.

Outcome: RTX reached a settlement and entered into a settlement agreement with the U.S. Department of State's Directorate of Defense Trade Controls. Includes 750 violations of the Arms Export Control Act (AECA), 22 U.S.C. § 2751 et seq., and the International Traffic in Arms Regulations (ITAR), 22 C.F.R. parts 120-130.

Dollar Impact: $200 million; $100 million of which RTX will use to fulfill its remedial obligations. RTX disclosed all of the alleged violations voluntarily. RTX also cooperated with the Department's review of this matter and has implemented numerous improvements to its compliance program since the conduct at issue.

GOVERNMENT CONTRACTING WEBCAST SERIES

ITAR Exemptions

BDO

ITAR Exemptions and Authorizations

Below are key ITAR exemptions and authorizations:

- General Applicability
- Exemptions for NATO and Major Non-NATO Allies
- Australia-UK-U.S. (AUKUS) Defense Trade Cooperation Treaties
- Dual/Third Country National Exception
- Technical Assistance Agreements (TAAs) and Manufacturing License Agreements (MLAs)

Exemptions of General Applicability

With certain exceptions, any of the following technical data (including classified information):

- To be disclosed pursuant to an official written request or directive from DoD
- Exported, reexported, or retransferred by or to a U.S. person, or a foreign person employee of a U.S. person travelling or on temporary assignment abroad, with restrictions
- In furtherance of a contract between the exporter and an agency of the U.S. Government, if the contract provides for the export of the data and such data does not disclose the details of design, development, production, or manufacture of any defense article
- Previously authorized for export to the same recipient
- Basic operations, maintenance, and training information relating to a defense article lawfully exported or authorized for export to the same recipient
- In the form of basic operations, maintenance, and training information relating to a defense article lawfully exported or authorized for export to the same recipient

22 C.F.R. § 125.4

Exemptions for NATO and Major Non-NATO Allies

EXEMPTION	REQUIRED CRITERIA	BUT NOT
No TAA is required for maintenance training or the performance of maintenance, including the export of supporting technical data for certain defense articles.	▶ Services must be for unclassified U.S.-origin defense articles lawfully exported or authorized for export and owned or operated by and in the relevant countries' inventory	▶ Any transaction involving defense services for which congressional notification is required
	▶ Includes inspection, testing, calibration or repair, including overhaul, reconditioning and one-to-one replacement of any defective items, parts or components	▶ Modification, enhancement, upgrade or other form of alteration or improvement that enhances the performance or capability of the defense article
	▶ Supporting technical data must be unclassified	▶ Any technical data for software documentation on the design or details of the computer software, software source code, design methodology, engineering analysis, or manufacturing know-how.

22 C.F.R. § 124.2

Australia-UK-U.S. (AUKUS) Defense Trade and Cooperation Treaties

EXEMPTION	SUBJECT TO THE FOLLOWING REQUIREMENTS
No license or other approval is required for the export, reexport, retransfer, or temporary import of defense articles, the performance of defense services, or engaging in brokering activities between or among authorized users of this exemption, subject to the requirements and limitations.	▶ The activity must be to or within the physical territory of Australia, the United Kingdom, or the United States ▶ Transferor, recipient, or broker must be registered with DDTC, a U.S. government agency, or a DDTC authorized user ▶ The defense article or defense service is not ineligible ▶ The value of the transfer is below certain maximums and does not involve the manufacturing abroad of SME ▶ Incorporation of certain terms in the commercial invoice

22 C.F.R. § 126.7

Certain Dual/Third Country Nationals Pt. 1

	Deemed Exports	Destination
EAR	Any release in the United States of technology or source code to a foreign person	The person's most recent country of citizenship or permanent residency
ITAR	Any release in the United States of ITAR-controlled technical data to a foreign person	Any country of citizenship or permanent residency held at any time, including those relinquished

Certain Dual/Third Country Nationals Pt. 2

With certain conditions, the three following scenarios:

22 C.F.R. § 126.18(a)

Transfer of unclassified defense articles, which includes technical data, to or within a foreign business entity, foreign governmental entity, or international organization that is an authorized end-user or consignee (including approved sub-licensees) for those defense articles, including the transfer to dual nationals or third-country nationals who are bona fide regular employees, directly employed by the foreign consignee or end-user.

22 C.F.R. § 126.18(d)

Reexport of unclassified defense articles or defense services to individuals who are dual national or third-country national employees of a foreign business entity, foreign governmental entity, or international organization, that is an authorized end-user, foreign signatory, or consignee (including approved sub-licensees) for those defense articles or defense services, when such individuals are regular employees, nationals of and physically within NATO and allied countries, sign an NDA, and are not the recipient of a permanent hardware transfer.

22 C.F.R. § 126.18(e)

Retransfer or reexport of classified defense articles to citizens of Australia or the United Kingdom, provided such individuals:

- are dual nationals of another country;
- are authorized users or regular employees of an authorized user of 126.7;
- hold a security clearance by Australia, UK, or the U.S. that is equivalent to SECRET or above; and
- Either: within the physical territory or a member of the armed forces acting in their official capacity.

MLAs and TAAs

Manufacturing License Agreements

- Agreement, approved by DDTC, whereby a U.S. person grants a foreign person an authorization to manufacture defense articles abroad and involves or contemplates:
  - (1) export of technical data or defense articles or the performance of a defense services, or
  - (2) the use by the foreign person of technical data or defense articles previously exported by the U.S. person.

Technical Assistance Agreements

- Agreement, approved by DDTC, that authorizes the furnishing of defense services or disclosing of technical data to foreign persons

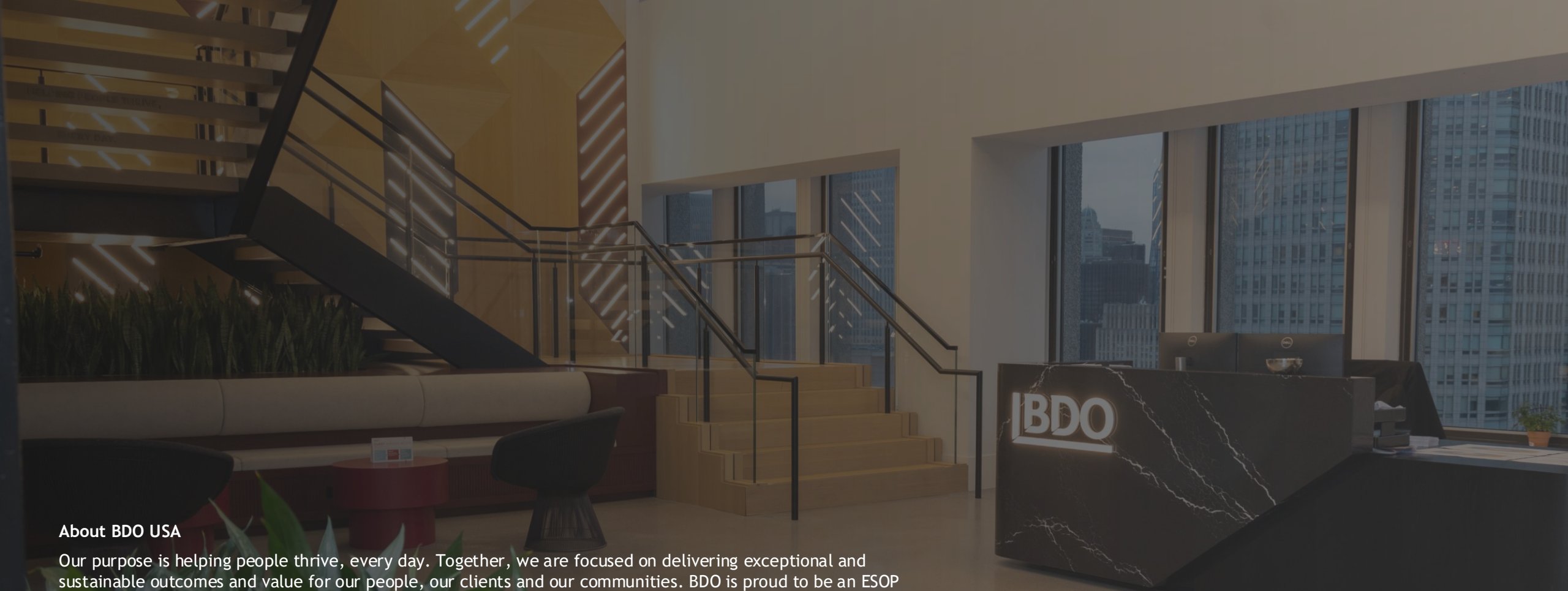
Timeline for Approval

- At least two months if not more after execution of the parties' contract

GOVERNMENT CONTRACTING WEBCAST SERIES

Questions?

BDO



About BDO USA

Our purpose is helping people thrive, every day. Together, we are focused on delivering exceptional and sustainable outcomes and value for our people, our clients and our communities. BDO is proud to be an ESOP company, reflecting a culture that puts people first. BDO professionals provide assurance, tax and advisory services for a diverse range of clients across the U.S. and in over 160 countries through our global organization.

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. For more information, please visit: www.bdo.com.

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

© 2025 BDO USA, P.C. All rights reserved.