Expanding CUI Regulations

How will this affect your organization?

FEBRUARY 19, 2025

With You Today

CHRISTINA REYNOLDS
Assurance Managing Director,
Government Contracting

629-401-6249
creynolds@bdo.com

BDO CMMC RPO Accredited Status

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

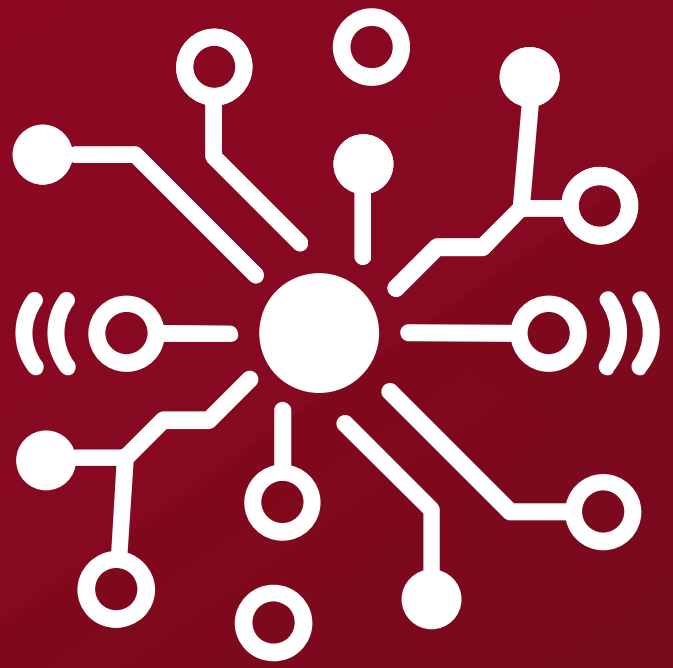
Source: [The Cyber AB: CMMC Accreditation]

Learning Objectives

Upon completion of this session, participants will be able to

- Identify new & emerging Federal Regulation for safeguarding of CUI
- Forecast for the emerging proposed rules for Federal & Department of Education
- Provide useful insights at NIST 800-171 & impacts to architecture design & cybersecurity

FAR 52.204-21: “Basic Cyber Hygiene” and FCI



FAR CLAUSE - FAR 52.204-21

Understanding “Basic Cyber Hygiene”

FAR 52.204-21:
Basic Safeguarding of Covered Contractor Information Systems

Defines FCI

Information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public websites) or simple transactional information, such as necessary to process payments.

Safeguarding

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

- Defines **“Basic Cyber Hygiene”**
- 15 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

What is CUI?

DFARS 252.204-7012

Safeguarding for Controlled Unclassified Information (CUI)

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

Defines CUI

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

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

Exemption: Manufacturers of COTS / Commercial Items

Provide "Adequate Security"
NIST SP 800-171

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

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

Mandatory 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)

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

Controlled Technical Information Examples:

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

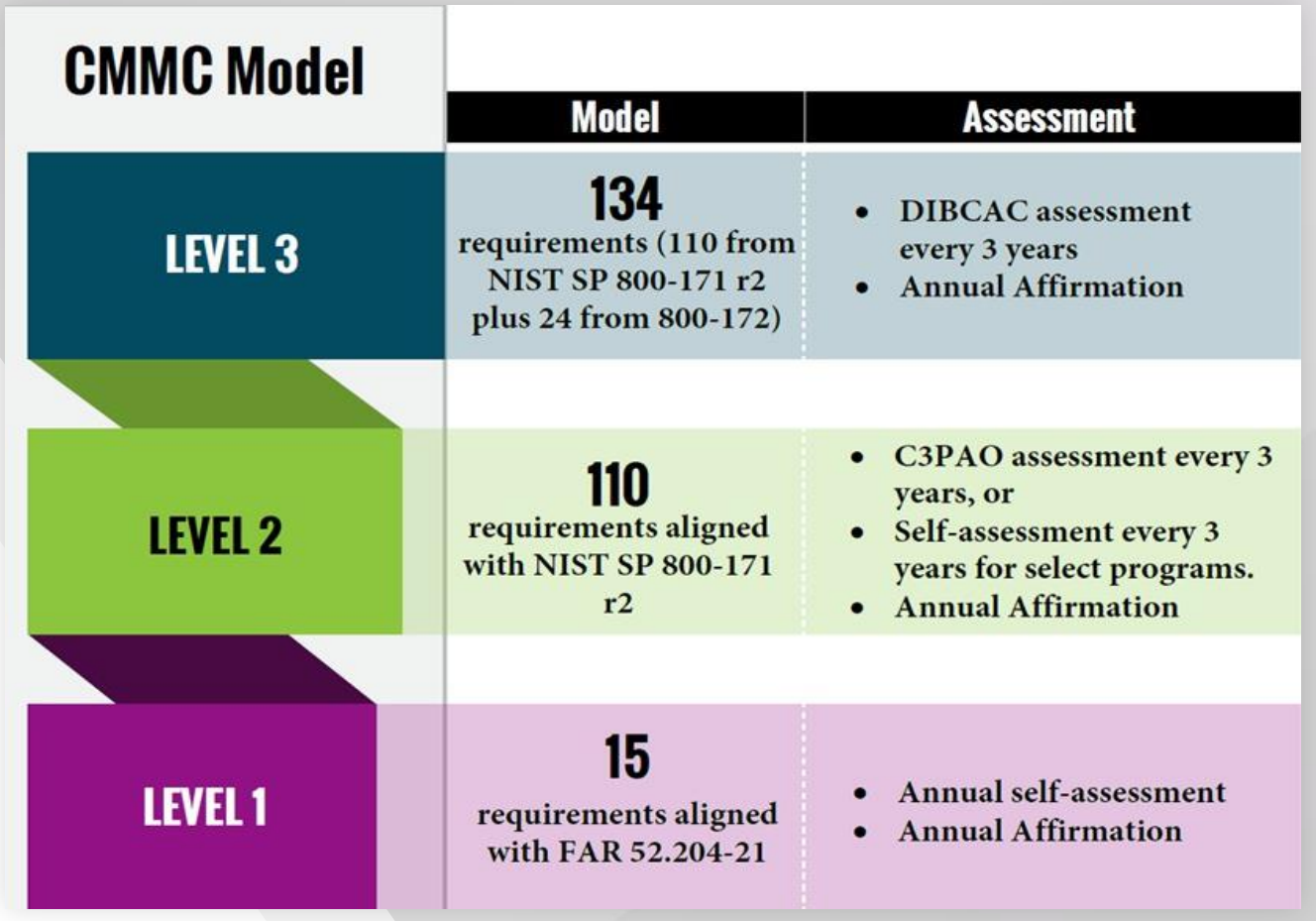
The Cybersecurity Maturity Model Certification (CMMC)

Updates for the CMMC 2.0 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 Processes



Source: CMMC Model (defense.gov)

CMMC 2.0 FINAL RULE

Key Takeaways

When will you see it in your contracts?

- **CMMC Contract clause:** DFARS 252.204-7021
  - Is a **Condition of Award** (must have at time of award to qualify for award)
  - Will appear in **new contracts & new option years**
- Defense contractors and subcontractors must comply with security requirements such as FAR clause 52.204-21 and DFARS clause 252.204-7012
- May also see related clauses in contract: DFARS clause 252.204-7019, 7020 and 7024
- Required to develop a **System Security Plan (SSP)**
- Defense contractors and subcontractors processing, storing, or transmitting **Federal Contract Information (FCI) are subject to CMMC Level 1**
- Defense contractors and subcontractors processing, storing, or transmitting **Controlled Unclassified Information (CUI) are subject to CMMC Level 2 or 3**
- The applicability of CMMC Level for procurement will be determined by the **Department of Defense (DoD)**
- Subcontractor flow-down is a requirement

CMMC 2.0 FINAL RULE

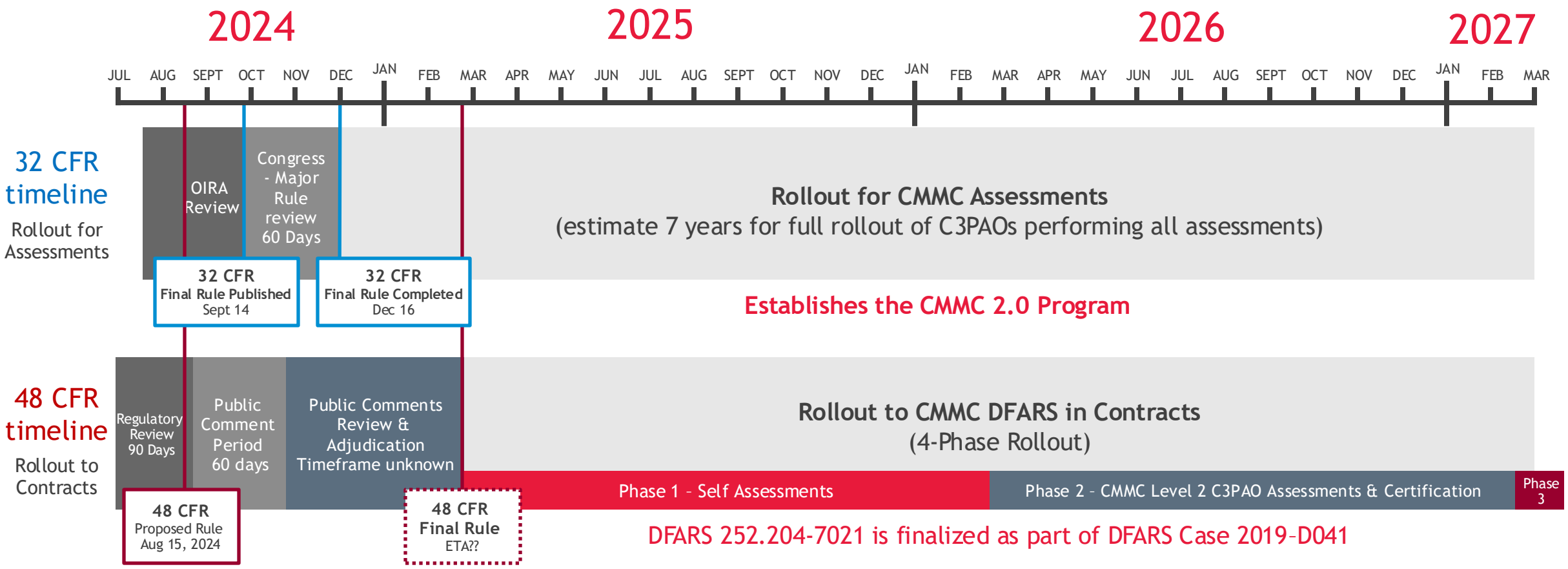
Key Takeaways

About CMMC 2.0

- Tiered Model (CMMC Levels 1-3):
  - **CMMC Level 1 (Self-Attest):**
    - Requires annual self-assessment and affirmation of security requirements by senior company official
  - **CMMC Level 2 (C3PAO Certification):**
    - Verification of security requirements aligned with NIST SP 800-171 Rev 2 is necessary for CMMC Level 2
  - **CMMC Level 3 (DoD Certification after Level 2 Certification):**
    - Must achieve CMMC Level 2 certification by C3PAO first
    - DIBCAC Certification of Level 3 after implementation of 24 selected security requirements from NIST SP 800-172
- Scores from self-assessments need to be submitted in the Department of Defense's Supplier Performance Risk System (SPRS). Post-3-year CMMC Certification, SPRS annual affirmations of compliance are mandatory yearly.
- Need to close out any Plan of Action and Milestones (POA&M) within 180 days of assessment

Current CMMC Rulemaking Timelines

Timelines are best estimates based on information publicly posted

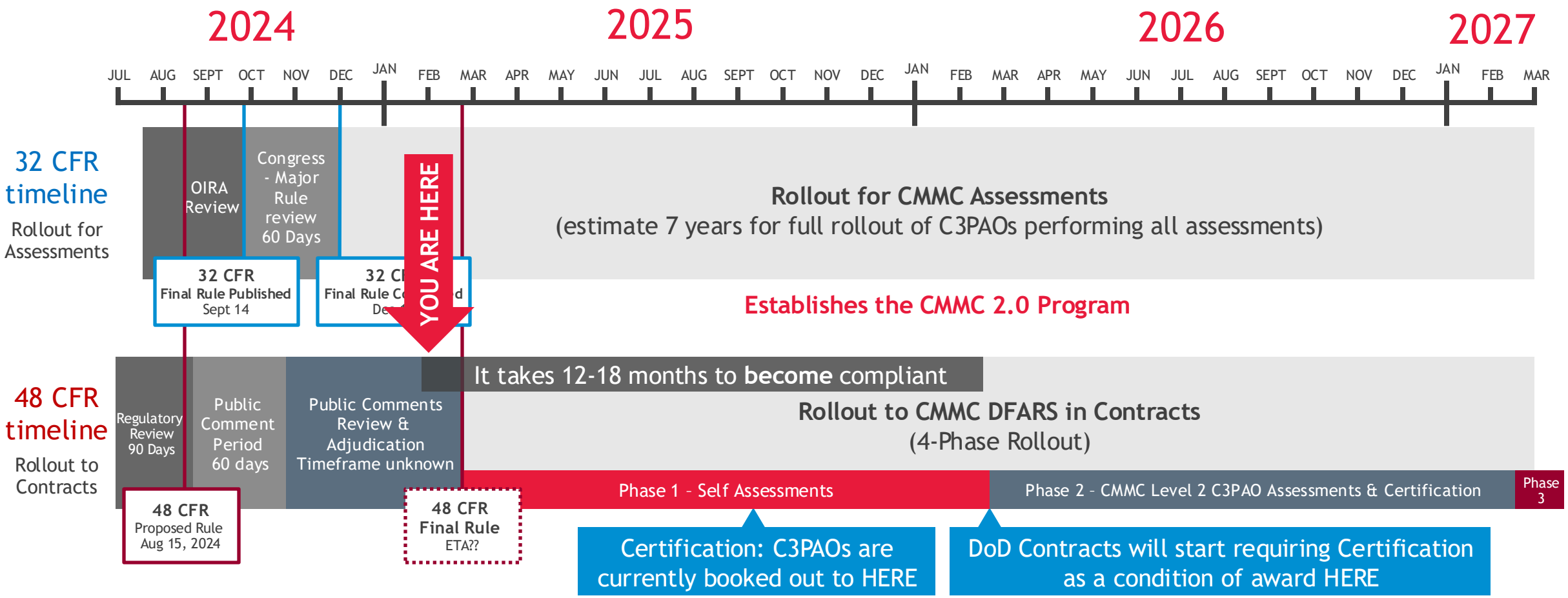


DoD will pursue rulemaking in:

1) title 32 of the Code of Federal Regulations (CFR), to establish the CMMC 2.0 program; and,
2) title 48 CFR, to implement any needed changes to the CMMC program content in 48 CFR.

Current CMMC Rulemaking Timelines

Timelines are best estimates based on information publicly posted



DoD will pursue rulemaking in:

1) title 32 of the Code of Federal Regulations (CFR), to establish the CMMC 2.0 program; and,
2) title 48 CFR, to implement any needed changes to the CMMC program content in 48 CFR.

CMMC Phased Implementation

In some procurements, DoD may implement CMMC requirements in advance of the planned phase

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

0-12 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.

12-24 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.

24-36 Months

Phase 4
Full Roll-out to all

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

36+ Months

*newly Changed for 32 CFR Final Rule

Other CUI Clauses

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

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

DON'T BE FOOLED

If You have ITAR, You have CUI

If you have DFARS 252.225-7048 "Export-Controlled Items" on your contract – assume 7012 is too

DFARS 252.225-7048 inserts requirements for export-controlled items under the contract. The Contractor shall comply with all applicable laws and regulations regarding export-controlled items, including, but not limited to, the requirement for contractors to register with the Department of State in accordance with 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:

1. The Export Administration Act of 1979, as amended (50 U.S.C. App. 2401, et seq.);
2. The Arms Export Control Act (22 U.S.C. 2751, et seq.);
3. The International Emergency Economic Powers Act (50 U.S.C. 1701, et seq.);
4. The Export Administration Regulations (15 CFR Parts 730-774);
5. The International Traffic in Arms Regulations (22 CFR Parts 120-130); and
6. Executive Order 13222, as extended.

FAR Proposed CUI Rule

New FAR Proposed Rule: DoD, GSA and NASA

POSTED 1/15/2025

CLICK HERE ►

Regulatory Background and Rule Overview

- The proposed FAR CUI Rule will require contractors and subcontractors across **all federal agencies** will be subject to more stringent CUI cybersecurity, training, and incident reporting requirements
  - Stakeholders: DoD, GSA, NASA
- The FAR CUI Rule proposes multiple changes to the FAR for standardizing CUI safeguarding, but its major components are:
  - **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
- **COTS Exemption remains:** 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

Background

- Executive Order 13556 – Obama Administration Nov 2010
  - Appointed NARA to implement uniform CUI program requirements for all federal contracts
  - 2016 - CUI program was codified in the Code of Federal Regulations at 32 C.F.R. Part 2002
  - Only the DoD has formalized contractual requirements directing contractors to safeguard CUI in accordance with 32 C.F.R. Part 2002
    - DFARS 252.204-7012
    - DFARS 252.204-7019/7020/7024
    - DFARS 252.204-7021 CMMC

PUBLISHED JAN 15, 2025

Proposed FAR CUI Rule

Creates two FAR Clauses:

FAR 52.204-XX

"Controlled Unclassified Information"
(when specified in the contract)

- Includes new form **Standard Form (SF) XXX** that the Govt provides to instruct on safeguarding/training for CUI specific to the contract
- Requires implementing NIST 800-171 **Revision 2**
- Report Cyber incidents **within 8 hours of discovery**
- Comply with any additional CUI safeguarding/ training requirements of SF-XXX form

FAR 52.204-YY

"Identifying and Reporting Information That Is Potentially Controlled Unclassified Information"

- This clause will apply if contractors receive a Standard Form indicating that they **will not handle or generate CUI** during contract performance
- Report to agencies if you have received information that may potentially be CUI and to report cyber incidents impacting such information
- If contractors receive CUI that is NOT reported on SF-XXX, you will have to report to the Gov within **8 hours**

FAR.204-XX

Information System Requirements

FAR 52.204-XX requires contractors to safeguard CUI according to:

a) Requirements set forth in 52.204-XX, and

b) Any additional, agency-specific CUI requirements, policies, or procedures that may be detailed in SF XXX.

The prescribed safeguarding requirements **only apply to CUI identified in SF XXX**.

Contractors who handle CUI within a non-federal (i.e., contractor) information system must:

- Comply with the 110 security requirements of NIST SP 800-171, Rev. 2
- Submit a system security plan (SSP) documenting its NIST SP 800-171, Rev. 2 compliance upon request by the government
- Implement additional information security requirements the contractor "reasonably determines" are necessary to provide adequate security for CUI
- If using a cloud service provider to handle or store CUI, ensure that the cloud provider meets Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline requirements and will comply with CUI incident reporting requirements
- Report the discovery of potential CUI to the government within 8 hours of discovery and safeguard the potential CUI until the government determines whether it is CUI or not

FAR.204-XX

Personnel Requirements

Federal Information Systems

- Applies to contractors who will handle CUI within a federal information system (a system owned by the Govt or operated on behalf of the Govt) to NIST SP 800-53
- Identified in the applicable SF XXX
- If using cloud computing services, must meet the FedRAMP Moderate baseline

Contractor-Owned Information Systems

- Provides general requirements for non-federal information systems
- Mandatory training for all personnel before they can access CUI
- Reporting suspected or confirmed incidents impacting CUI to the Government within **eight hours of discovery**
- Flowing down CUI to subcontractors where subcontract performance involves CUI

FAR 52.204-YY

Contracts Without Identified CUI

FAR 52.204-YY will apply where the applicable SF XXX indicates that contractors will not receive or generate CUI during contract performance.

- **If CUI is discovered:** Must notify the applicable contracting officer (CO) within 8 hours of discovery if they discover information that they believe or have reason to know is CUI.
  - The contractor must "appropriately safeguard" the information until the CO determines whether the information at issue is CUI or not.
  - This may mean that you need an appropriate encrypted storage mechanism or secure network even if you think you won't receive CUI.
- **Proprietary Information:** Contractors must identify the information they own and provide to the government, such as proprietary business information, so that the government can determine what should be protected as CUI.
- **Cyber Incident:** If a CUI incident occurs, the government may release information provided by contractors for limited purposes, such as national security. The government will only release such information to the extent necessary.
- **Flowdown:** Clause 52.204-YY must be flowed down to all subcontractors in its entirety.
- **Incidents:** Under 52.204-YY, contractors must notify the relevant CO if they discover a potential CUI incident, i.e., an event involving the improper access, use, disclosure, modification, or destruction of potential CUI, and inventory the potential CUI involved in the incident. **The CO must be notified within 8 hours of incident discovery.**

Submit Your Comments Now

Submit comments in response to FAR Case 2017-016 to the Federal eRulemaking portal at https://www.regulations.gov by searching for "FAR Case 2017-016". Select the link "Comment Now" that corresponds with "FAR Case 2017-016". Follow the instructions provided on the "Comment Now" screen.

Please include your name, company name (if any), and "FAR Case 2017-016" on your attached document. If your comment cannot be submitted using https://www.regulations.gov, call or email the points of contact in the **FOR FURTHER INFORMATION CONTACT** section of this document for alternate instructions.

Instructions

Please submit comments only and cite "FAR Case 2017-016" in all correspondence related to this case.

SF-XXX:

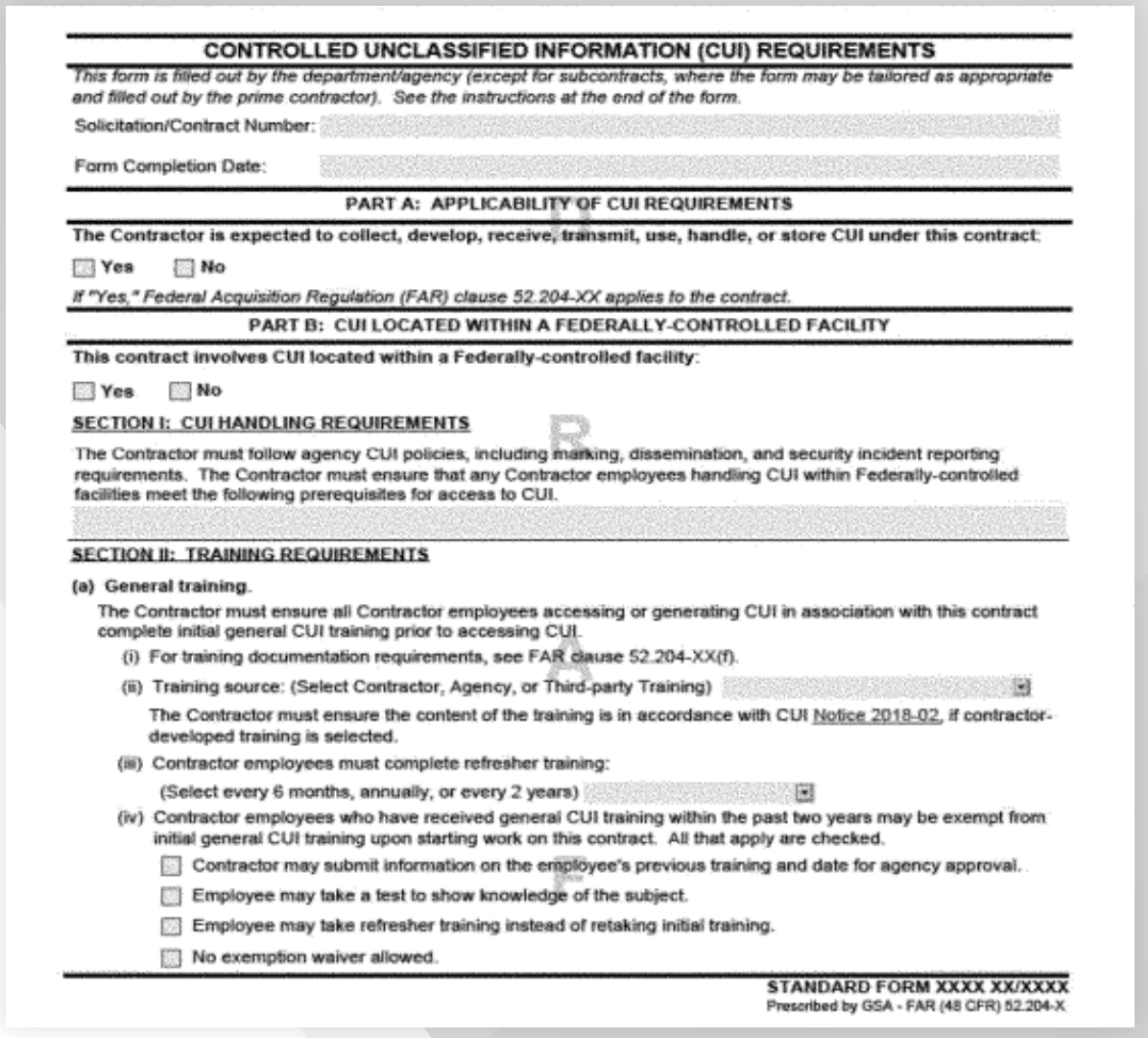
The Contract Form for Disclosure of CUI in the Contract

The Standard Form SF XXX

- The rule introduces a new mechanism, the Standard Form (SF) XXX, Controlled Unclassified Information Requirements
- Agencies will be required to use the Standard Form (SF XXX) in solicitations and contracts that may involve CUI
- While the contracting agency will provide SF XXX to prime contractors, higher tier contractors are responsible for generating and providing an SF XXX for each subcontract they expect to involve CUI
- The SF XXX must identify the category or categories of CUI that the contractor may handle or generate during performance
- Contractors are only required to use safeguards for the CUI specified in the form but may have additional reporting responsibilities under FAR 52.204-XX or FAR 52.204-YY if they discover potential CUI not identified in SF XXX

SF XXX

Standard Form for CUI



CONTROLLED UNCLASSIFIED INFORMATION (CUI) REQUIREMENTS

This form is filled out by the department/agency (except for subcontracts, where the form may be tailored as appropriate and filled out by the prime contractor). See the instructions at the end of the form.

Solicitation/Contract Number:

Form Completion Date:

PART A: APPLICABILITY OF CUI REQUIREMENTS

The Contractor is expected to collect, develop, receive, transmit, use, handle, or store CUI under this contract:

☐ **Yes** ☐ **No**

If "Yes," Federal Acquisition Regulation (FAR) clause 52.204-XX applies to the contract.

PART B: CUI LOCATED WITHIN A FEDERALLY-CONTROLLED FACILITY

This contract involves CUI located within a Federally-controlled facility:

☐ **Yes** ☐ **No**

SECTION I: CUI HANDLING REQUIREMENTS

The Contractor must follow agency CUI policies, including marking, dissemination, and security incident reporting requirements. The Contractor must ensure that any Contractor employees handling CUI within Federally-controlled facilities meet the following prerequisites for access to CUI.

SECTION II: TRAINING REQUIREMENTS

(a) General training.

The Contractor must ensure all Contractor employees accessing or generating CUI in association with this contract complete initial general CUI training prior to accessing CUI.

(i) For training documentation requirements, see FAR clause 52.204-XX(f).

(ii) Training source: (Select Contractor, Agency, or Third-party Training)

The Contractor must ensure the content of the training is in accordance with CUI Notice 2018-02, if contractor-developed training is selected.

(iii) Contractor employees must complete refresher training:

(Select every 6 months, annually, or every 2 years)

(iv) Contractor employees who have received general CUI training within the past two years may be exempt from initial general CUI training upon starting work on this contract. All that apply are checked.

☐ Contractor may submit information on the employee's previous training and date for agency approval.

☐ Employee may take a test to show knowledge of the subject.

☐ Employee may take refresher training instead of retaking initial training.

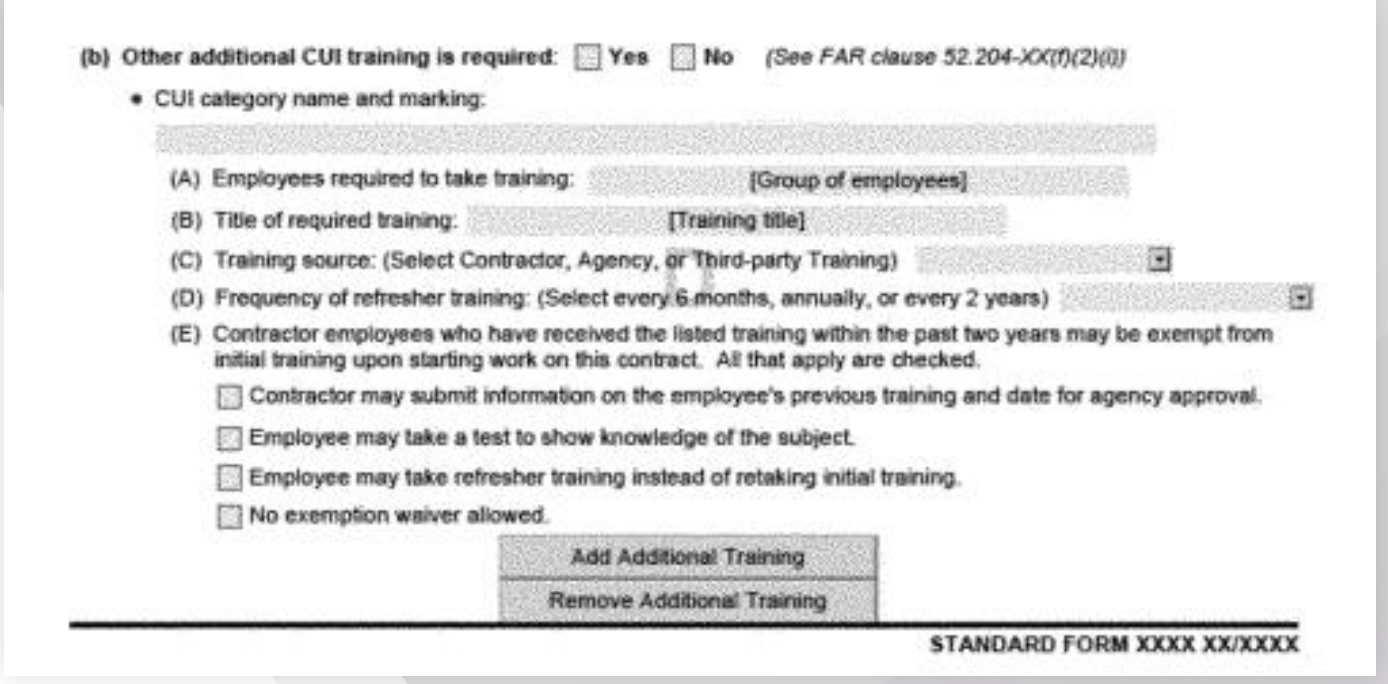
☐ No exemption waiver allowed.

STANDARD FORM XXXX XX/XXXX

Prescribed by GSA - FAR (48 CFR) 52.204-X

SF XXX

Standard Form for CUI



(b) Other additional CUI training is required: ☐ Yes ☐ No *(See FAR clause 52.204-XX(f)(2)(i))*

- CUI category name and marking:

(A) Employees required to take training: [Group of employees]

(B) Title of required training: [Training title]

(C) Training source: (Select Contractor, Agency, or Third-party Training)

(D) Frequency of refresher training: (Select every 6 months, annually, or every 2 years)

(E) Contractor employees who have received the listed training within the past two years may be exempt from initial training upon starting work on this contract. All that apply are checked.

☐ Contractor may submit information on the employee's previous training and date for agency approval.

☐ Employee may take a test to show knowledge of the subject.

☐ Employee may take refresher training instead of retaking initial training.

☐ No exemption waiver allowed.

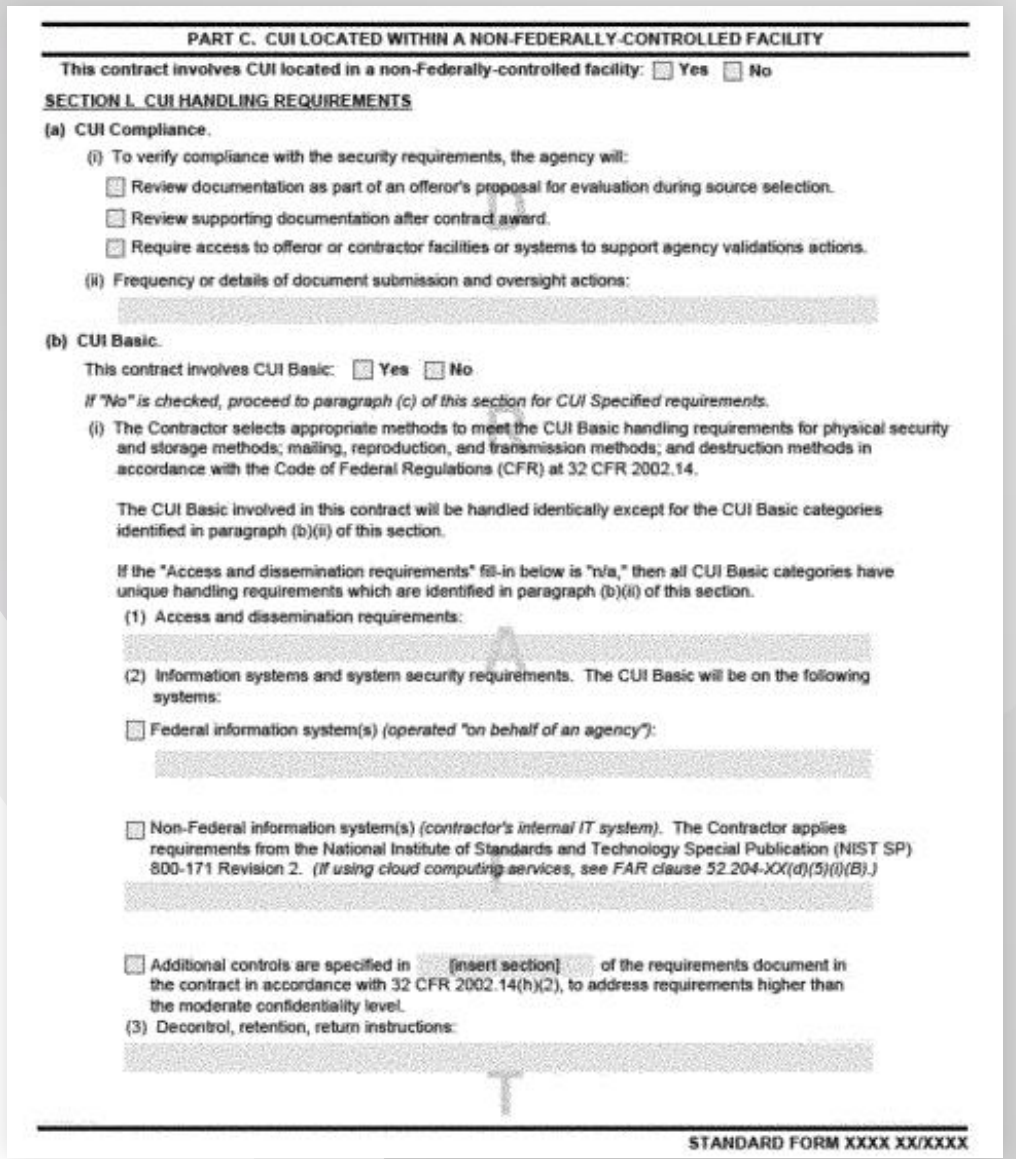
Add Additional Training

Remove Additional Training

STANDARD FORM XXXX XX/XXXX

SF XXX

Standard Form for CUI



PART C. CUI LOCATED WITHIN A NON-FEDERALLY-CONTROLLED FACILITY

This contract involves CUI located in a non-Federally-controlled facility: ☐ Yes ☐ No

SECTION I. CUI HANDLING REQUIREMENTS

(a) CUI Compliance.

(i) To verify compliance with the security requirements, the agency will:

☐ Review documentation as part of an offeror's proposal for evaluation during source selection.

☐ Review supporting documentation after contract award.

☐ Require access to offeror or contractor facilities or systems to support agency validations actions.

(ii) Frequency or details of document submission and oversight actions:

(b) CUI Basic.

This contract involves CUI Basic: ☐ Yes ☐ No

If "No" is checked, proceed to paragraph (c) of this section for CUI Specified requirements.

(i) The Contractor selects appropriate methods to meet the CUI Basic handling requirements for physical security and storage methods; mailing, reproduction, and transmission methods; and destruction methods in accordance with the Code of Federal Regulations (CFR) at 32 CFR 2002.14.

The CUI Basic involved in this contract will be handled identically except for the CUI Basic categories identified in paragraph (b)(ii) of this section.

If the "Access and dissemination requirements" fill-in below is "n/a," then all CUI Basic categories have unique handling requirements which are identified in paragraph (b)(ii) of this section.

(1) Access and dissemination requirements:

(2) Information systems and system security requirements. The CUI Basic will be on the following systems:

☐ Federal information system(s) *(operated "on behalf of an agency")*:

☐ Non-Federal information system(s) *(contractor's internal IT system)*. The Contractor applies requirements from the National Institute of Standards and Technology Special Publication (NIST SP) 800-171 Revision 2. *(If using cloud computing services, see FAR clause 52.204-XX(d)(5)(i)(B).)*

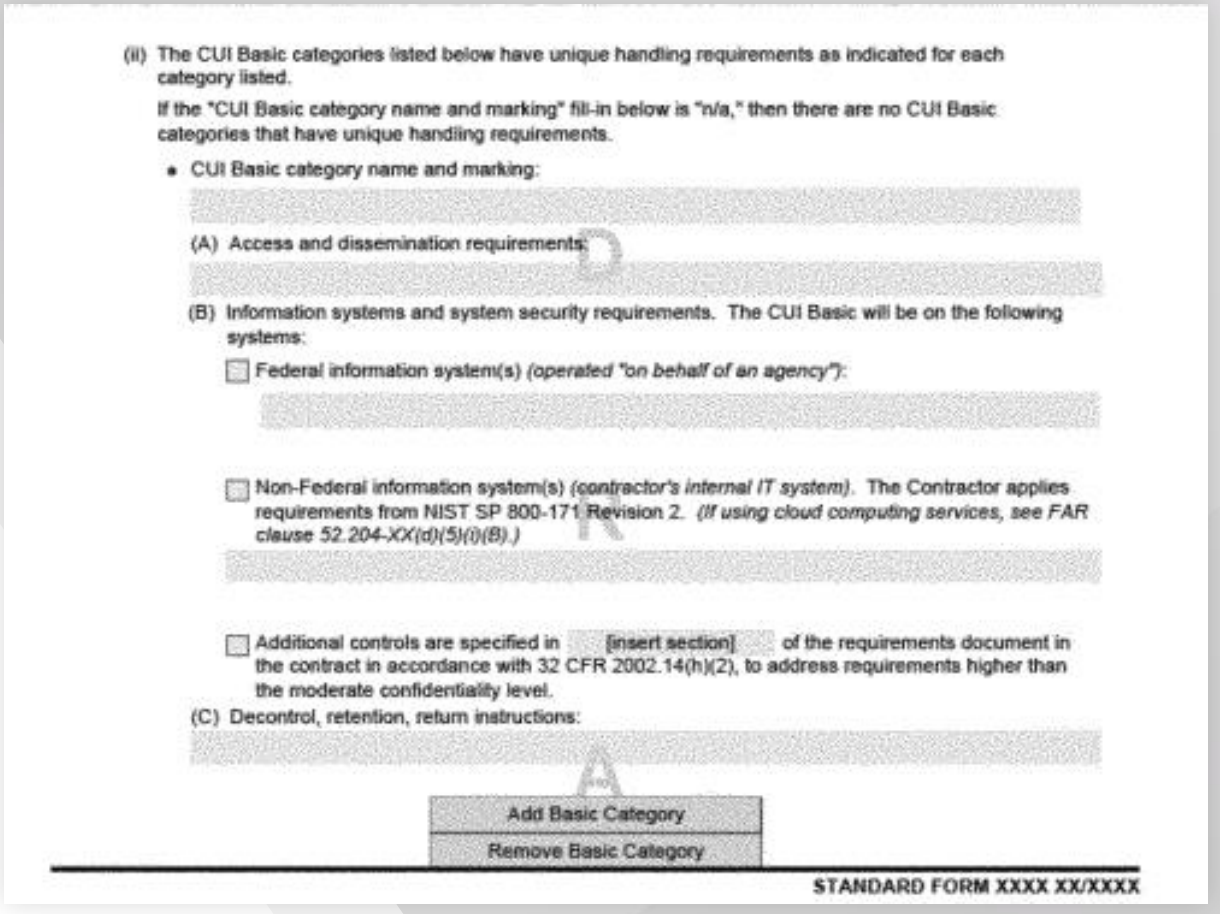
☐ Additional controls are specified in [insert section] of the requirements document in the contract in accordance with 32 CFR 2002.14(h)(2), to address requirements higher than the moderate confidentiality level.

(3) Decontrol, retention, return instructions:

STANDARD FORM XXXX XX/XXXX

SF XXX

Standard Form for CUI



(ii) The CUI Basic categories listed below have unique handling requirements as indicated for each category listed.

If the "CUI Basic category name and marking" fill-in below is "n/a," then there are no CUI Basic categories that have unique handling requirements.

- CUI Basic category name and marking:

(A) Access and dissemination requirements:

(B) Information systems and system security requirements. The CUI Basic will be on the following systems:

☐ Federal information system(s) *(operated "on behalf of an agency")*:

☐ Non-Federal information system(s) *(contractor's internal IT system)*. The Contractor applies requirements from NIST SP 800-171 Revision 2. *(If using cloud computing services, see FAR clause 52.204-XX(d)(5)(i)(B).)*

☐ Additional controls are specified in [insert section] of the requirements document in the contract in accordance with 32 CFR 2002.14(h)(2), to address requirements higher than the moderate confidentiality level.

(C) Decontrol, retention, return instructions:

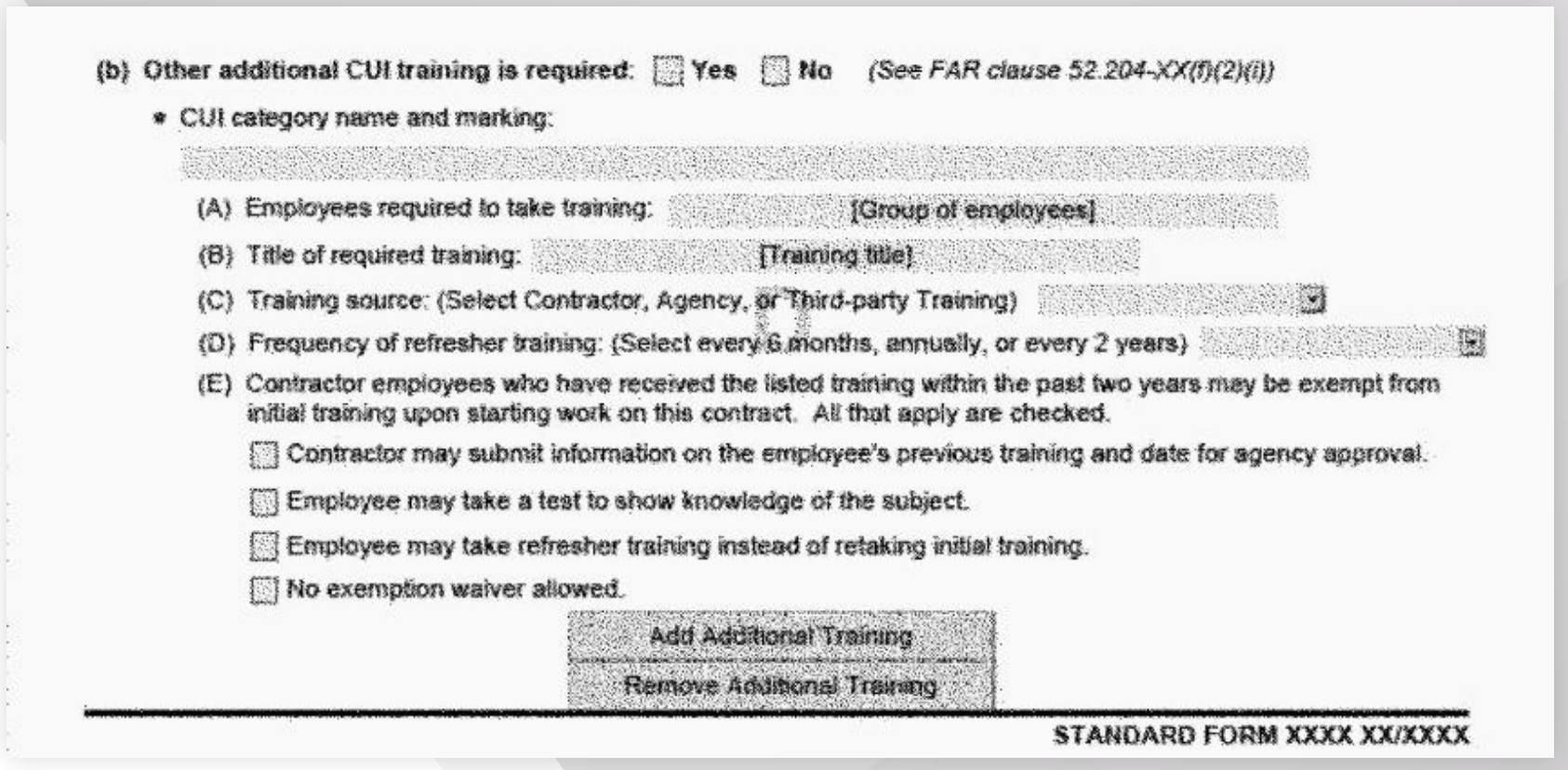
Add Basic Category

Remove Basic Category

STANDARD FORM XXXX XX/XXXX

SF XXX

Standard Form for CUI



(b) Other additional CUI training is required: ☐ Yes ☐ No *(See FAR clause 52.204-XX(f)(2)(i))*

- CUI category name and marking:

(A) Employees required to take training: [Group of employees]

(B) Title of required training: [Training title]

(C) Training source: (Select Contractor, Agency, or Third-party Training)

(D) Frequency of refresher training: (Select every 6 months, annually, or every 2 years)

(E) Contractor employees who have received the listed training within the past two years may be exempt from initial training upon starting work on this contract. All that apply are checked.

☐ Contractor may submit information on the employee's previous training and date for agency approval.

☐ Employee may take a test to show knowledge of the subject.

☐ Employee may take refresher training instead of retaking initial training.

☐ No exemption waiver allowed.

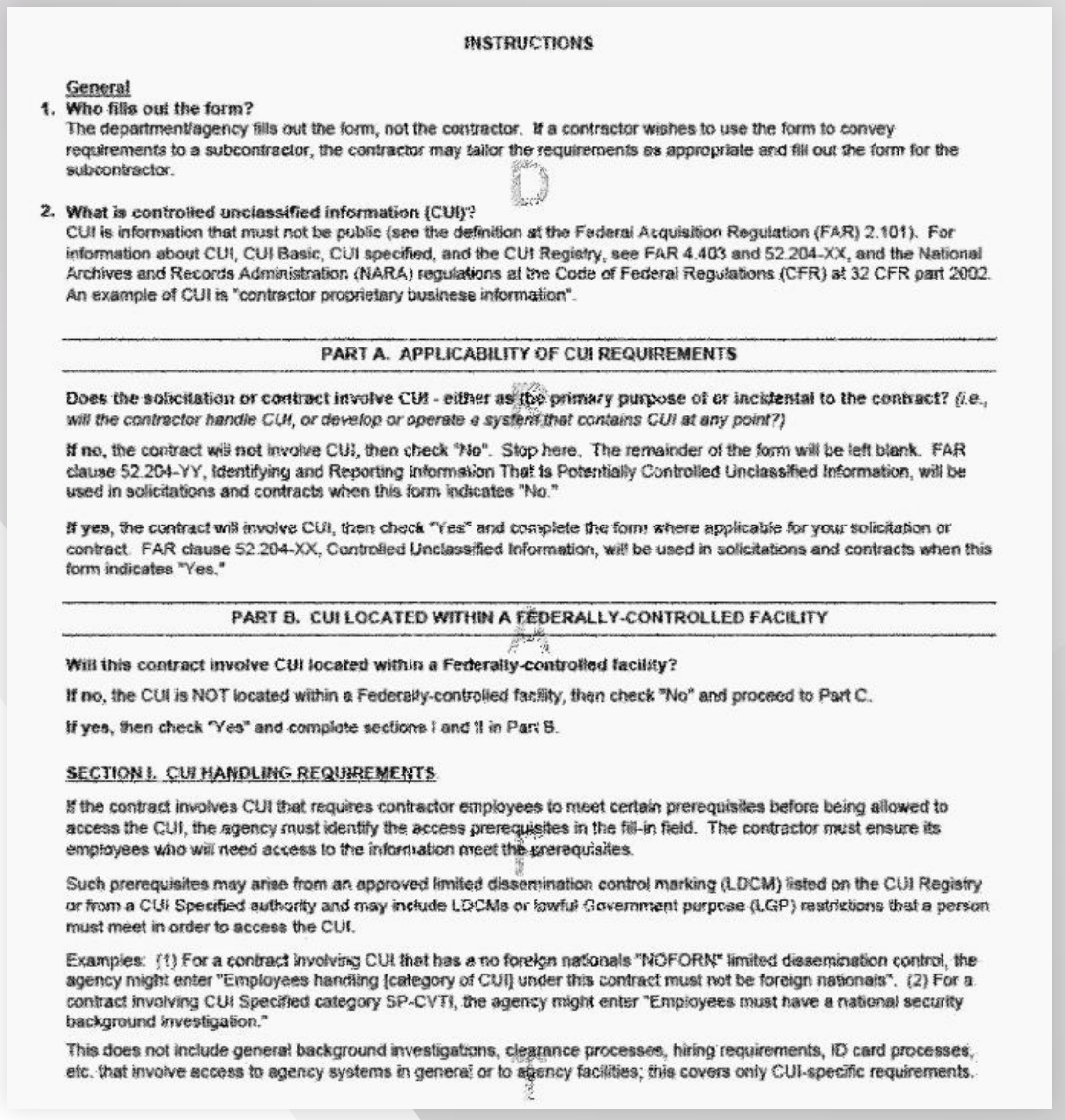
Add Additional Training

Remove Additional Training

STANDARD FORM XXXX XX/XXXX

SF XXX

Standard Form for CUI



INSTRUCTIONS

General

1. **Who fills out the form?**
The department/agency fills out the form, not the contractor. If a contractor wishes to use the form to convey requirements to a subcontractor, the contractor may tailor the requirements as appropriate and fill out the form for the subcontractor.

2. **What is controlled unclassified information (CUI)?**
CUI is information that must not be public (see the definition at the Federal Acquisition Regulation (FAR) 2.101). For information about CUI, CUI Basic, CUI specified, and the CUI Registry, see FAR 4.403 and 52.204-XX, and the National Archives and Records Administration (NARA) regulations at the Code of Federal Regulations (CFR) at 32 CFR part 2002. An example of CUI is "contractor proprietary business information".

PART A. APPLICABILITY OF CUI REQUIREMENTS

Does the solicitation or contract involve CUI - either as the primary purpose of or incidental to the contract? *(i.e., will the contractor handle CUI, or develop or operate a system that contains CUI at any point?)*

If no, the contract will not involve CUI, then check "No". Stop here. The remainder of the form will be left blank. FAR clause 52.204-YY, Identifying and Reporting Information That is Potentially Controlled Unclassified Information, will be used in solicitations and contracts when this form indicates "No."

If yes, the contract will involve CUI, then check "Yes" and complete the form where applicable for your solicitation or contract. FAR clause 52.204-XX, Controlled Unclassified Information, will be used in solicitations and contracts when this form indicates "Yes."

PART B. CUI LOCATED WITHIN A FEDERALLY-CONTROLLED FACILITY

Will this contract involve CUI located within a Federally-controlled facility?

If no, the CUI is NOT located within a Federally-controlled facility, then check "No" and proceed to Part C.

If yes, then check "Yes" and complete sections I and II in Part B.

SECTION I. CUI HANDLING REQUIREMENTS

If the contract involves CUI that requires contractor employees to meet certain prerequisites before being allowed to access the CUI, the agency must identify the access prerequisites in the fill-in field. The contractor must ensure its employees who will need access to the information meet the prerequisites.

Such prerequisites may arise from an approved limited dissemination control marking (LDCM) listed on the CUI Registry or from a CUI Specified authority and may include LDCMs or lawful Government purpose (LGP) restrictions that a person must meet in order to access the CUI.

Examples: (1) For a contract involving CUI that has a no foreign nationals "NOFORN" limited dissemination control, the agency might enter "Employees handling [category of CUI] under this contract must not be foreign nationals". (2) For a contract involving CUI Specified category SP-CVTI, the agency might enter "Employees must have a national security background investigation."

This does not include general background investigations, clearance processes, hiring requirements, ID card processes, etc. that involve access to agency systems in general or to agency facilities; this covers only CUI-specific requirements.

SF XXX

Standard Form for CUI

SECTION II. TRAINING REQUIREMENTS.

(a) Provide general CUI training information.

(i) All contractor employees must take general CUI training prior to accessing CUI. They must also complete refresher training not less often then once every two years.

(ii) Identify the source for the general CUI training (i.e., contractor may develop its own training, contractor must use agency training, or contractor may use training developed by third parties).

(iii) Select from the drop-down the appropriate frequency for refresher training (i.e., every 6 months, annually, or every 2 years).

(iv) If the agency will allow contractor employees to be exempt from the requirement for initial general CUI training when they have received such training in a previous job, check the applicable methods the agency will allow contractor employees to use (i.e., submit employee training details, employee testing, or refresher training) to demonstrate proficiency. If the exemption waiver is not allowed, check the last box.

(b) Provide other additional CUI training information.

If the agency requires some or all contractor employees to take additional training in accordance with FAR 52.204-XX(f)(2)(i), check "Yes" and complete the information. If there are no additional training requirements, check "No."

Enter the CUI category name and marking that requires additional training in the fill-in field.

(A) Enter the group of contractor employees who must take the training by title, the office they will work in, or other identifier.

(B) Enter the title of the additional training they must take.

(C) Select the training source from the drop-down for the additional training (i.e., contractor may develop its own training, contractor must use agency training, or contractor may use training developed by third parties).

(D) Select from the drop-down box the frequency with which contractor employees must re-take this additional training.

(E) If the agency will allow contractor employees to be exempt from the initial additional training requirement, identify the methods the agency will allow contractor employees to use to demonstrate proficiency by checking the appropriate box(es) (i.e., submit employee training details, employee testing, or refresher training). If an exemption waiver is not allowed, check the last box.

Use the "Add Additional Training" button to create an entry for each CUI category.

PART C. CUI LOCATED WITHIN A NON-FEDERALLY-CONTROLLED FACILITY

Will this contract involve CUI located within a non-Federally-controlled facility?

If no, the CUI is NOT located within a non-Federally-controlled facility, then check "No". Stop here; the remaining sections in Part C will not be applicable.

If yes, then check "Yes" and complete sections I through IV.

SECTION I. CUI HANDLING REQUIREMENTS.

(a) Identify which method(s) will be used to verify compliance. Determine which method(s) the agency will use to verify the contractor is complying with the contract's security requirements.

(i) Check one or more of the boxes that apply at (a)(i) "To verify compliance with the security requirements, the agency will."

(ii) Using the fill-in field under paragraph(a)(ii), enter how often (annually, every six months, etc.) the contractor will need to submit verifying documents, the details of document submission, and the type of oversight actions the agency will engage in.

Department of Education Proposed CUI Rule

New Department of Education Proposed Rule

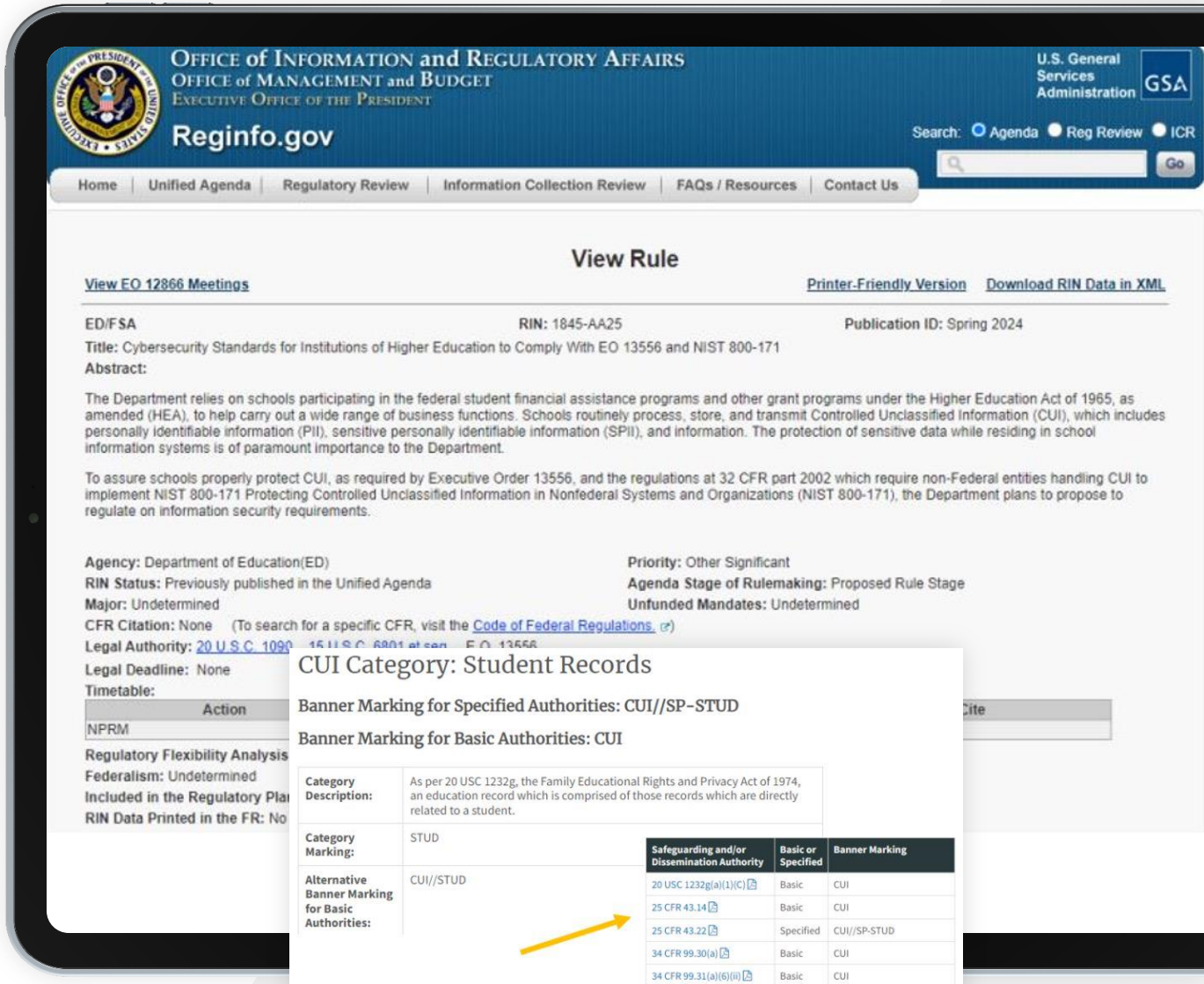
"The Department relies on schools participating in the federal student financial assistance programs and other grant programs under the Higher Education Act of 1965, as amended (HEA), to help carry out a wide range of business functions.

Schools routinely process, store, and transmit Controlled Unclassified Information (CUI), which includes personally identifiable information (PII), sensitive personally identifiable information (SPII), and information.

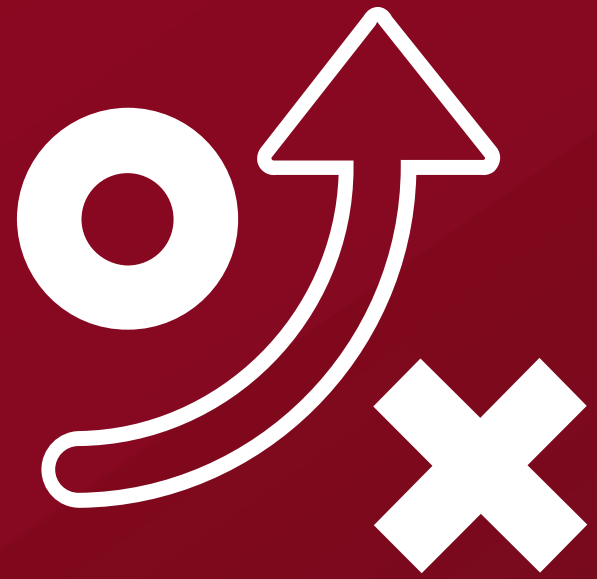
The protection of sensitive data while residing in school information systems is of paramount importance to the Department.

To assure schools properly protect CUI, as required by Executive Order 13556, and the regulations at 32 CFR part 2002 which require non-Federal entities handling CUI to implement NIST 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (NIST 800-171), the Department plans to propose to regulate on information security requirements."

Source: RIN: 1845-AA25



What do you need to do?



Things a Contractor Can Do to Prepare for CUI Clauses

Scoping

- Know what clauses are in your current contracts
- Look ahead - Know what the agencies you **want to contract with** may have for CUI clauses before you bid
- Know what CUI you have on your systems currently and where those files are stored and shared
- Know who in your organization has access to these files
- Know what systems you store them on – not all systems are compliant

Prepare & Plan

- Are your systems NIST 800-171 compliant? What is your current score?
- Do you need to build a new CUI enclave? Can you buy an inherited SaaS environment (PreVeil, Box.com, Kiteworks etc.)?
- If you are on Microsoft Commercial – know that it is not compliant, and you will need to consider GCC/ GCC High
- If you are on Google, you will need to consider the Google Gov platform or an overlay SaaS solution
- Are you storing CUI in your ERP/Business Systems? You need to know before planning your architecture

Things a Contractor Can Do to Prepare for CUI Clauses

Ask Questions

- When the RFP has a Q&A session – ask questions!
- Will DFARS 7012 or DFARS 7021 be put on this Contract?
- Will this contract be exempt from DFARS 7012/7021 due to [COTS items or Commercial Items]
- Will CMMC certification be required as a condition of award?
- Until the new FAR clause comes out – ask for the **Security Classification Guide** (once the FAR comes out, the SF-XXX form will take its place)

Don't Fail to Plan for Contingencies & Incidents

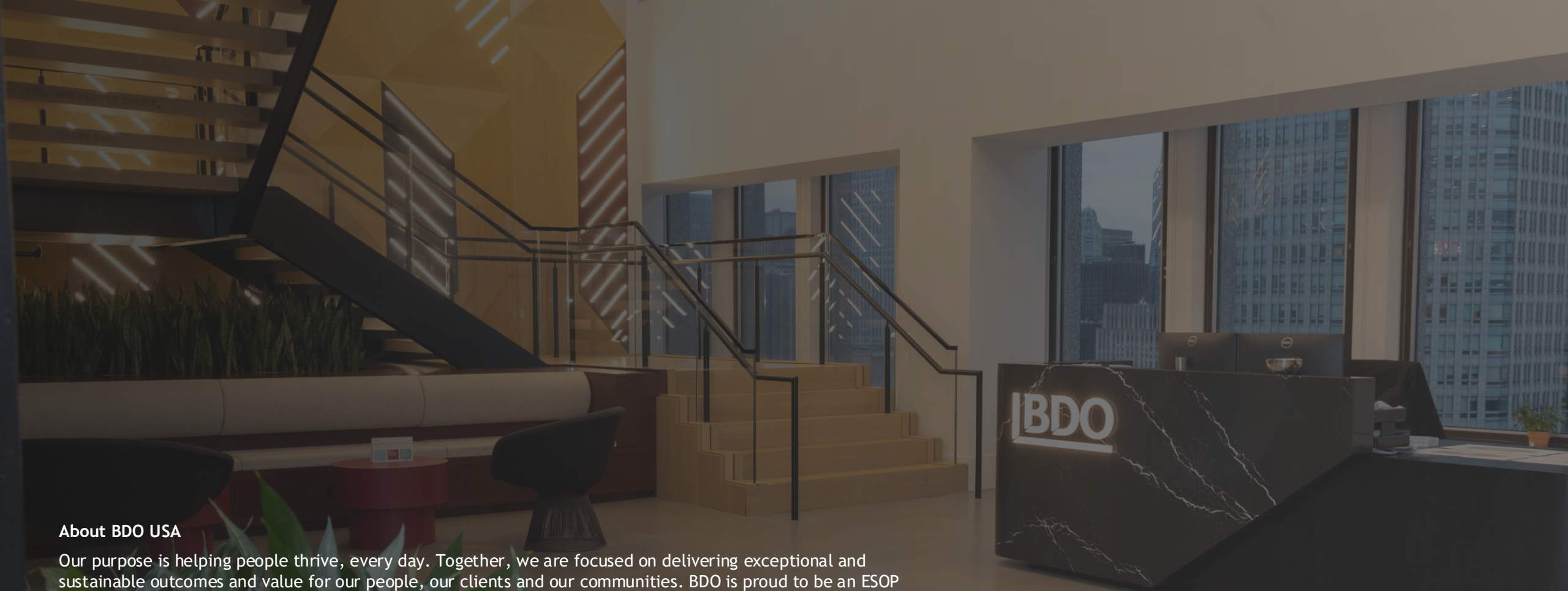
- Even if you get a FAR 52.204-YY, that does not mean you will never see CUI
- You may receive CUI at any time so have a backup plan (PreVeil is a great option for this)
- Receive all email for any Federal/DoD contracts through a secured address – do not assume the Government knows where to safely send you CUI – they will send to the address they have on file
- Put a header on your lower security side emails to prevent accidental CUI spills to unsecured systems: **"This email is not approved for the receipt or processing of CUI. To send CUI to [company] please address it to [secure-email@company.us]"**

Questions?

Save the date for our next Government Contracting Webcast

- Thursday, March 20, 2025
- 11:00 AM – 12:00 PM ET
- **Handling ITAR & Export Control Data: Exceptions for Existing Agreements & Cybersecurity Implications**
- Join Christina Reynolds of BDO USA and Erica Bakies with Seyfarth Shaw LLP as they discuss the complex landscape of Cybersecurity Maturity Model Certification (CMMC) and Controlled Unclassified Data (CUI) and the intricacies of CUI and US Data sovereignty withing the International Traffic in Arms Regulations (ITAR).
- Register today!

1.0 CPE Credit In the field of Information Technology (IT)



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.