DEPARTMENT OF DEFENSE

GENERAL SERVICES ADMINISTRATION

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

48 CFR Parts 1, 2, 3, 4, 5, 7, 9, 11, 12, 15, 27, 33, 42, 52, and 53

[FAR Case 2017–016, Docket No. 2017–0016, Sequence No. 1]

RIN 9000–AN56

Federal Acquisition Regulation: Controlled Unclassified Information

AGENCY: Department of Defense (DoD), General Services Administration (GSA), and National Aeronautics and Space Administration (NASA).

ACTION: Proposed rule.

SUMMARY: DoD, GSA, and NASA are proposing to amend the Federal Acquisition Regulation (FAR) to implement the National Archives and Records Administration's Controlled Unclassified Information Program enacted under an Executive Order entitled Controlled Unclassified Information.

DATES: Interested parties should submit written comments to the Regulatory Secretariat Division at the address shown below on or before March 17, 2025 to be considered in the formation of the final rule.

ADDRESSES: 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. Public comments may be submitted as an individual, as an organization, or anonymously (see frequently asked questions at *https://www.regulations.gov/faq*). Comments submitted in response to this rule will be made publicly available and are subject to disclosure under the Freedom of Information Act. For this reason, please do not include in your comments information of a confidential nature, such as sensitive personal information or proprietary information, or any information that you would not want publicly disclosed unless you follow the instructions below for confidential comments. Summary information of the public comments received, including any specific comments, will be posted on *https://www.regulations.gov.*

All filers using the portal should use the name of the person or entity submitting comments as the name of their files, in accordance with the instructions below. Anyone submitting business confidential/proprietary information should clearly identify any business confidential/proprietary portion at the time of submission, file a statement justifying nondisclosure and referencing the specific legal authority claimed, and provide a non-confidential/non-proprietary version of the submission. Any business confidential information should be in an uploaded file that has a file name beginning with the characters ''BC.'' Any page containing business confidential information must be clearly marked ''BUSINESS CONFIDENTIAL/PROPRIETARY'' on the top of that page.

The corresponding non-confidential/non-proprietary version of those comments must be clearly marked ''PUBLIC.'' The file name of the non-confidential version should begin with the character ''P.'' The ''BC'' and ''P'' should be followed by the name of the person or entity submitting the comments or rebuttal comments. All filers should name their files using the name of the person or entity submitting the comments. Any submissions with file names that do not begin with a ''BC'' will be assumed to be public and will be made publicly available through *https://www.regulations.gov.*

To confirm receipt of your comment(s), please check *https://www.regulations.gov,* approximately two-to-three days after submission to verify posting.

FOR FURTHER INFORMATION CONTACT: For clarification of content, contact Mr. Michael O. Jackson, Procurement Analyst, at 202–821–9776 or by email at *michaelo.jackson@gsa.gov.* For information pertaining to status, publication schedules, or alternate instructions for submitting comments if *https://www.regulations.gov* cannot be used, contact the Regulatory Secretariat Division at 202–501–4755 or *GSARegSec@gsa.gov.* Please cite FAR Case 2017–016.

SUPPLEMENTARY INFORMATION:

I. Background

Today, Federal information and information systems are increasingly the targets of sophisticated attacks by criminals and our adversaries, as well as subject to risks involving non-adversarial threats (*e.g.,* accidental misuse of information). Executive Order (E.O.) 13556, *Controlled Unclassified Information,* established the Controlled Unclassified Information (CUI) Program to manage information that requires safeguarding or dissemination controls and designated the National Archives and Records Administration (NARA) as the executive agent of the CUI Program.

NARA published a final rule on September 14, 2016 (81 FR 63324) to implement the CUI requirements of E.O. 13556. As part of the implementation of the NARA final rule, NARA maintains a registry (*https://www.archives.gov/cui*) of unclassified information that requires safeguarding or dissemination controls. NARA's CUI Registry identifies the organizational index grouping and related categories of information and specifies how the information should be marked and disseminated, among other actions that must be taken.

NARA's rule codified uniform policies and procedures for marking, safeguarding, disseminating, decontrolling, and disposing of CUI for Federal executive branch agencies at 32 CFR part 2002. These policies also affect contractors that are expected to collect, develop, receive, transmit, use, handle, or store CUI during contract performance. To apply the policies to contractors, the CUI Program must be incorporated into the acquisition process, specifically, when agencies define their requirements, issue solicitations, and award contracts. In order to do so, Government and contractor roles and responsibilities for safeguarding, using, marking, disseminating, and decontrolling CUI residing on both Federal and non-Federal information systems must be identified.

DoD has implemented the requirements of the CUI Program within the clause at Defense Federal Acquisition Regulation Supplement (DFARS) 252.204–7012, Safeguarding Covered Defense Information and Cyber Incident Reporting. DoD has also proposed amending the DFARS to incorporate contractual requirements associated with the Cybersecurity Maturity Model Certification program (CMMC) in order to verify contractor implementation of security controls through a proposed rule published in the **Federal Register** on August 15, 2024, at 89 FR 66327. Separately, the CMMC program was established in Title 32 of the Code of Federal Regulations through a final rule published in the

Federal Register on October 15, 2024, at 89 FR 83092.

DoD, GSA, and NASA are proposing to revise the FAR to implement NARA's final rule on the Federal CUI Program as it relates to performance under Federal contracts. The Privacy Act requirements at FAR part 24 are not changed by this rulemaking.

DoD, GSA, and NASA propose to create a common mechanism, the Standard Form XXX, Controlled Unclassified Information (CUI) Requirements, to enable a uniform process for communicating the information contractors must manage and safeguard as well as identify where a CUI incident must be reported and when there are CUI incident reporting requirements that differ from or are in addition to those in the clause at FAR 52.204–XX(g). Currently laws, Federal regulations, and Government-wide policies already mandate these protections, but there is not a standard way these requirements are identified and shared with contractors.

This proposed rule is just one element of a larger strategy to improve the Government's efforts to identify, deter, protect against, detect, and respond to increasingly sophisticated criminals and adversaries targeting Federal information and information systems.

II. Discussion and Analysis

The proposed rule introduces a new standard form (SF) to support uniformity in Governmentwide implementation of these policies. It identifies roles and responsibilities for agencies and contractors when controlled unclassified information (CUI) is located on Federal information systems within a Federal facility or resides on or transits through contractor information systems or within contractor facilities, and it adds two new clauses and a provision to enable contractor reporting and compliance responsibilities in Federal solicitations and contracts.

The proposed rule is intended to provide for the following:

(1) SF XXX, Controlled Unclassified Information (CUI) Requirements, was developed to promote consistency, assist Federal agencies and contractors in the identification of CUI in agency requirements, and uniformly define all associated handling requirements in accordance with 32 CFR part 2002. The SF XXX will be included in solicitations and contracts that may result in the handling of CUI that will ultimately become performance requirements during contract performance.

(2) FAR 2.101 definitions for ''contractor-attributional information,'' ''controlled unclassified information (CUI),'' ''CUI incident,'' and ''CUI Registry'' are added to provide clarification as these terms are new to the FAR. The definition of ''information system'' is moved from FAR subpart 4.19 to 2.101. The term ''Federally-controlled information system'' is updated to ''Federal information system.''

(3) FAR 3.104–4 is amended to clarify that certain information must be marked by the contractor before submitting it to the Government (contractor bid or proposal information, contractor-attributional information, contractor proprietary business information, and source selection information). Contracting officers should consult with the contractor if they are unsure whether information provided by the contractor falls into one of these categories. Contracting officers who are unsure how to handle such information, including whether it is CUI, should consult with agency officials as necessary.

(4) FAR subpart 4.4:

- The subpart heading is revised to read ''Safeguarding Information and Information Systems'' since the information referred to in subpart 4.4 is not limited to classified information and now includes CUI.
- Section 4.401 is amended to add a definition for ''information'' which was moved and revised from the definition currently at FAR 4.1901.
- At FAR 4.403 and 4.404, the current content is moved to FAR 4.402.
- FAR 4.403 is replaced with new content that provides instructions on the implementation of the CUI Program. The added language identifies the contracting officer's role in receiving and incorporating the SF XXX in solicitations and contracts and the contracting officer's responsibilities during contract administration. A new provision at FAR 52.204–WW, Notice of Controlled Unclassified Information Requirements, and new clauses at FAR 52.204–XX, Controlled Unclassified Information, and 52.204–YY, Identifying and Reporting Information That Is Potentially Controlled Unclassified Information, are also prescribed. The changes for FAR 4.403 include the following:
  - Existing FAR 4.403 has been renumbered as FAR 4.402–2.
  - The clause at FAR 4.404 was moved to a new FAR 4.402–3.
  - FAR 4.403–1 adds definitions for ''CUI Basic,'' ''CUI categories,'' ''CUI Specified,'' ''handling,'' ''lawful Government purpose,'' ''limited dissemination control,'' and ''on behalf of an agency.''
  - FAR 4.403–2 provides information on E.O. 13556 including that the E.O. establishes NARA as the executive agent for the CUI Program.
  - FAR 4.403–3 gives the applicability of the SF XXX and the new FAR clauses 52.204–XX and 52.204–YY.
  - FAR 4.403–4 outlines the CUI policy and requires that CUI involved in performance of a contract shall be identified on a SF XXX and incorporated into the contract. Unmarked or mismarked CUI is not considered a CUI incident unless the mismarking or lack of marking has resulted in the mishandling or improper dissemination of the information. Offerors are requested and contractors are required to notify the Government within an 8 hour timeframe if they discover or suspect information is CUI, but that CUI is not listed on an SF XXX or is not marked or properly marked.
  - FAR 4.403–5 adds the usage of the SF XXX. The SF XXX itself has detailed instructions.
  - FAR 4.403–6 provides that the agency point of contact to whom the contractor reports an incident is found in the SF XXX at Part C, Section IV. When the SF XXX is not used in a contract, the point of contact is identified in FAR 52.204–YY(b). FAR 4.403–6 explains that the SF XXX should list any special incident reporting requirements for CUI Specified. FAR 4.403–6 also adds that the contracting officer shall provide instructions to the contractor for submitting the system images, in accordance with agency procedures. FAR 4.403–6 also explains that the contractor is required to hold the system images for 90 days unless the Government declines interest.
  - FAR 4.403–7 requires the contracting officer to insert the clause at FAR 52.204–XX, Controlled Unclassified Information, or the clause at FAR 52.204–YY, Identifying and Reporting Information That Is Potentially Controlled Unclassified Information, and to insert the provision at FAR 52.204–WW, Notice of Controlled Unclassified Information Requirements, in solicitations and contracts, excluding solicitations and contracts solely for the acquisition of commercially available off-the-shelf (COTS) items.
- FAR 4.404 clause prescription is moved to FAR 4.403–7. Coverage from FAR subpart 4.19 has been moved to FAR 4.404.
- Several organizational changes, including relocation of text and definitions from FAR subpart 4.19, improve the logical flow of information.

• FAR 4.404–1 adds definitions for ''covered contractor information system'' and ''covered Federal information.'' The term ''Federal contract information'' was changed to ''covered Federal information'' to align with the term ''covered contractor information system,'' and the definition of ''covered Federal information'' was revised to clarify that the term excludes CUI and classified information. The definition of ''covered Federal information'' is also amended in FAR clause 52.204–21, Basic Safeguarding of Covered Contractor Information Systems.

• FAR 4.404–2, Applicability, has been added to state that while covered Federal information is not required to be marked or identified by the Government, some administrative markings (*e.g.,* draft, deliberative process, predecisional, not for public release) can indicate that the information is covered Federal information.

• FAR 4.404–3 has been added to require the contracting officer to insert the clause at FAR 52.204–21, Basic Safeguarding of Covered Contractor Information Systems, in solicitations and contracts, excluding solicitations and contracts solely for the acquisition of COTS items or Federally-funded basic and applied research in science, technology, and engineering at colleges, universities, and laboratories in accordance with National Security Decision Directive 189 when the agency does not provide any covered Federal information to the contractor. FAR 4.404–3 replaces the clause prescription section at FAR 4.1903. The prescription for the clause at FAR 52.204–21 was updated to match the prescription for the CUI clause, because, while both types of information are likely to be in a wide range of contracts, covered Federal information is more ubiquitous than CUI and it may be difficult for the contracting officer to identify during development of the solicitation when covered Federal information may be applicable for the procurement.

• FAR 4.1301 and 4.1303 have been updated to remove the references to ''PUB Number'' and ''PUB'' and edit the term ''Federally-controlled information system'' to make it ''Federal information system''.

(5) FAR 7.103, Agency-head responsibilities. New language is added to describe agency planners' responsibilities for compliance with 32 CFR part 2002 and the completion of the SF XXX during acquisition planning.

(6) FAR 7.105, Contents of written acquisition plans. CUI is added to the security considerations to be addressed during acquisition planning.

(7) At FAR 7.503, Policy, language has been revised to clarify that the list of examples of functions generally not considered to be inherently governmental functions, includes contractors working in any situation that permits or might permit them to gain access to CUI.

(8) FAR subpart 9.5, Organizational and Consultant Conflicts of Interest, includes updates to FAR 9.505, 9.505–4, and 9.508 to make clear proprietary information is contractor proprietary business information.

(9) FAR 11.002, Policy. New language is added to incorporate the requirements for CUI and use of the SF XXX when describing agency needs.

(10) FAR 12.202, Market research and description of agency need. New language is added to incorporate the requirements for CUI and the SF XXX in requirements documents for the acquisition of commercial products and commercial services.

(11) At FAR 15.407–1, a reference to CUI and classified information is added to clarify the type of information that should be protected from improper disclosure.

(12) At FAR subpart 15.6, conforming changes are made to change ''proprietary information'' and ''restrictive legend'' or ''legend'' to ''contractor proprietary business information'' and ''administrative marking,'' respectively.

(13) FAR 27.203, Security requirements for patent applications and other patent information. A new section is added to inform contracting officers that CUI safeguarding requirements apply to patent application and other patent information.

(14) FAR part 52. A new provision FAR 52.204–WW, Notice of Controlled Unclassified Information Requirements, is added to inform offerors of requirements on restricted use of Government-provided information, on appropriately identifying sensitive offeror-provided information, and on notifying the Government regarding unmarked or mismarked CUI. A new FAR clause 52.204–XX, Controlled Unclassified Information, is added to require contractors to comply with applicable CUI requirements, if the SF XXX indicates that the contractor is expected to collect, develop, receive, transmit, use, handle, or store CUI under the contract. A new FAR clause 52.204–YY, Identifying and Reporting Information That Is Potentially Controlled Unclassified Information, is added to apply to contracts in which the requiring activity indicates on the SF XXX that no CUI is involved in the performance of the contract. CUI requirements include:

• Requirements for how the contractor must mark CUI submitted to the Government and notify the Government of any mismarked or unmarked CUI discovered;

• Restrictions on the contractor's use of Government-provided information apply whether or not the information is marked as CUI;

• Requirements for safeguarding CUI residing on Federal and non-Federal systems, as identified in the SF XXX, Controlled Unclassified Information (CUI) Requirements;

• Requirements for reporting and managing security incidents;

• Actions that may be necessary to validate compliance;

• Minimum CUI training requirements; and

• The requirement for contractors to flow down CUI requirements to subcontractors, if applicable.

(15) FAR 52.204–21, Basic Safeguarding of Covered Contractor Information Systems. Text is added for the definition and at paragraph (b)(3) for the identification of ''covered Federal information''.

(16) FAR clause 52.212–5 is updated to reflect that FAR clause 52.204–XX is applicable to acquisitions of commercial products and services. FAR clause 52.213–4 is updated to reflect usage of the FAR 52.204–XX clause in simplified acquisitions for other than commercial products or services. FAR clause 52.244–6 is updated to address the flow down to subcontracts for the two new clauses.

(17) Additional minor edits are made at FAR 1.106 to add the OMB control number information for the provision and clause, at FAR 42.302 to update a cross-reference, and at FAR subpart 53.2 to add the new SF XXX, Controlled Unclassified Information (CUI) Requirements.

III. Applicability to Contracts at or Below the Simplified Acquisition Threshold (SAT) and for Commercial Products, Including Commercially Available Off-the-Shelf (COTS) Items, or Commercial Services

This rule proposes a new provision at FAR 52.204–WW, Notice of Controlled Unclassified Information Requirements. The proposed provision is prescribed at FAR 4.403–7(a) for use in solicitations that contain the clause at FAR 52.204–XX or the clause at FAR 52.204–YY. The rule proposes a new clause at FAR 52.204–XX, Controlled Unclassified Information. The proposed clause is

prescribed at FAR 4.403–7(b) for use in solicitations and contracts if the requiring activity has marked the ''Yes'' box in Part A of the SF XXX, except for solicitations and contracts solely for the acquisition of COTS items. The rule proposes a new clause at FAR 52.204–YY, Identifying and Reporting Information That Is Potentially Controlled Unclassified Information. The proposed clause is prescribed at FAR 4.403–7(c) for use in solicitations and contracts if the requiring activity has marked the ''No'' box in Part A of the SF XXX, excluding solicitations and contracts solely for the acquisition of COTS items.

This rule also proposes to amend the FAR to implement 32 CFR part 2002, Controlled Unclassified Information, in Federal solicitations and contracts. The objective of the rule is to implement uniform, Governmentwide policies and procedures for Federal agencies and contractors regarding handling of CUI. Since CUI requires protection regardless of dollar value or commerciality of the product or service, this rule will apply to contracts at or below the SAT and to commercial products and commercial services. The rule does not apply to contracts that are solely for the acquisition of COTS items.

IV. Expected Impact of the Rule

A. General Compliance Requirements

Under the terms of this proposed rule, contractors will be required to safeguard CUI that the Government identifies in the standard form (SF) XXX, Controlled Unclassified Information (CUI) Requirements, and ensure handling consistent with 32 CFR part 2002. This includes CUI that the agency provides to the contractor, or CUI that the contractor collects, develops, receives, transmits, uses, handles, or stores in performance of the contract. CUI is defined at FAR 2.101 as information that the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Governmentwide policy requires or permits an agency to handle using safeguarding or dissemination controls.

The contractor shall permit access to CUI only as described in the SF XXX. A contractor will need to review the SF XXX to determine what information under the contract is considered CUI and how to properly safeguard the CUI. If the contractor intends to flow CUI down to a subcontractor, then the contractor will also be required to prepare an SF XXX and distribute it to the subcontractor to ensure the subcontractor properly safeguards CUI. Any contractor or subcontractor employee that handles CUI will be required to complete training on safeguarding CUI, as specified on the SF XXX.

Identification of CUI on the SF XXX triggers compliance requirements as specified in the new contract clause at FAR 52.204–XX, Controlled Unclassified Information, *e.g.,* security requirements in NIST SP 800–171, Revision 2, or controls in NIST SP 800–53 depending on the type of information systems that process, store, or transmit CUI. The compliance requirements are discussed in more detail in section IV.C. of this preamble and will vary depending on the organizational Index Grouping and category of CUI being handled under the contract and how the information is being collected, developed, received, transmitted, used, handled, or stored. Prime contractors that flow down CUI to subcontractors will also be required to flow down the compliance requirements of the clause at FAR 52.204–XX; a requirement that applies at all subcontract tiers. The new clause at FAR 52.204–YY also flows down to subcontracts.

A new solicitation provision at FAR 52.204–WW, Notice of Controlled Unclassified Information Requirements, is prescribed for use in solicitations that contain the new clause at FAR 52.204–XX or the new clause at FAR 52.204–YY. This provision provides a notice to offerors that agencies will provide agency procedures on handling CUI during the solicitation phase if handling CUI is necessary to prepare an offer. The notice also advises offerors that contractor bid or proposal information, proprietary business information, or contractor-attributional information must be properly marked to ensure adequate protection of their information. The provision also advises offerors that they should notify the contracting officer if there appears to be unmarked or mismarked CUI or an incident related to CUI handled by the offeror during the solicitation phase.

When the contract does not identify CUI, the new contract clause at FAR 52.204–YY, Identifying and Reporting Information That Is Potentially Controlled Unclassified Information, is used in lieu of the CUI clause. Similar to the solicitation provision, this clause requires the contractor to notify the Government if there appears to be unmarked or mismarked CUI or a suspected CUI incident related to information handled by the contractor in performance of the contract. This clause requires the contractor to properly mark proprietary business information or contractor-attributional information to ensure adequate protection.

The new solicitation provision and the new contract clauses all forbid an offeror or contractor from using Government-provided information for its own purposes, whether or not the information is marked as CUI, unless the information is in the public domain, or unless the information is lawfully made available to the offeror or contractor by someone other than the Government.

B. Benefits

1. Uniform Cybersecurity Hygiene Baseline

Establishing uniform requirements for how the acquisition workforce and Federal contractors manage CUI will significantly improve the Government and Federal contractors' ability to protect Federal information and information systems from criminals and our adversaries. Absent the uniform approach proposed in this rule, agencies will continue to employ ad hoc, agency-specific policies to manage this information, an approach that can cause agencies to mark and handle information inconsistently and inefficiently. While waivers may be applied in some circumstances, this rule is intended to establish a Governmentwide baseline that will lead to more effective implementation of protections for this sensitive information by the acquisition workforce and contractors. More effective implementation of requirements for identifying and marking CUI will reduce scenarios in which contractors may not realize the information that they are handling is sensitive information that must be safeguarded.

2. Protection From Potential Financial Impacts of CUI Incidents

Failure to adopt these basic cybersecurity requirements can have a substantial financial impact on a business. There have been many analyses regarding the cost of cybersecurity incidents and the estimates vary widely. In order to establish a defensible set of cost and loss data that is suitable for the analysis of cybersecurity incident costs in the Federal sector, the Cyber Security and Infrastructure Security Agency (CISA) Office of the Chief Economist (OCE), in the Department of Homeland Security, reviewed a broad range of cyber cost and loss studies and presented an analysis of the per-incident, aggregate, and scenario-based estimates of cyber loss. On October 26, 2020, the CISA

OCE released a report with the results of their analyses and a summary of per-incident loss estimates available in the most widely cited published research, commercial datasets, and industry reports. OCE estimated the median cost of a cybersecurity incident cited in the surveyed publications ranged from $0.5 to $1.6 million. The maximum cost per incident cited ranged from $11.7 million to greater than $1 billion. The CISA OCE acknowledges in its report that the differences in the assumptions, approaches to data collection, and specific incidents included in the datasets for the above sources result in a high degree of variability among the loss estimates.[1]

3. Increased Protection of Sensitive Information

Given the potential financial impacts a CUI incident may have on companies and individuals, it is imperative that Federal contractors who are entrusted with sensitive information in the performance of Government contracts adopt the basic cybersecurity hygiene requirements outlined in this rule. This increased baseline of cybersecurity hygiene across Federal contractors will reduce the number of incidents that have the potential to place sensitive information at risk and pose serious threats to individuals, Federal operations and assets, and the contractors themselves. For the remaining incidents that may occur, the requirement for contractors to report suspected or confirmed CUI incidents within 8 hours, unless a different time period is required for a specific category of CUI or a Federally-controlled facility, will allow the Federal Government to have appropriate situational awareness, quickly respond to the incident, and reduce the impact of the event.

C. Public Costs

The total estimated public costs associated with this FAR rule in billions over a 10-year period are as follows:

Public cost	Undiscounted	2 Percent
Present Value	$17.63	$15.89
Annualized	1.76	1.77

Undiscounted public costs (in billions) by year over the 10-year period are summarized as follows:

Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Year 8	Year 9	Year 10
$2.28	$1.71	$1.71	$1.71	$1.71	$1.71	$1.71	$1.71	$1.71	$1.71

The following is a summary from the Regulatory Impact Analysis (RIA) of the specific compliance requirements and the estimated costs of compliance. The new FAR clause is modeled after the most recent version of the clause at DFARS 252.204–7012, which introduced many of these compliance requirements on defense contractors and subcontractors in 2015 and required compliance not later than December 31, 2017. Therefore, the estimated costs of compliance have been segregated into those that are new for Federal offerors, contractors, and subcontractors (see section IV.C.1 of this preamble) and those that are new only for non-defense contractors and subcontractors (see section IV.C.2 of this preamble). The RIA includes a detailed discussion and explanation about the assumptions and methodology used to estimate the cost of this regulatory action, including the specific impact and costs for small businesses. Public comment is requested on the RIA, which is available at *https://www.regulations.gov* (search for ''FAR Case 2017–016,'' click ''Open Docket,'' and view ''Supporting Documents'').

1. Federal Offerors, Contractors, and Subcontractors

The following compliance requirements are considered new for Federal offerors, contractors, and subcontractors required to safeguard CUI:

a. Regulatory Familiarization

Familiarization accounts for the time to read and understand the rule. It is expected that most contractors will be required to become familiar with the various compliance requirements of the FAR, in order to be prepared to handle or receive CUI in performance of a Federal contract. According to award data in the Federal Procurement Data System (FPDS) for fiscal year (FY) 2021 through FY 2023, on average per year the Government awards contracts and orders for supplies and services to 67,547 unique contractors, all of whom are expected to become familiar with this rule. It is estimated that on average it will take two hours per contractor and subcontractor that handle CUI to review the rule. The estimated cost for regulatory familiarization in the first year of implementation is $10,267,144 (67,547 contractors and subcontractors * 2 hours/entity * $76/hour), of which $6,711,104 is attributed to 44,152 small businesses.

b. Review the SF XXX

Offerors, contractors, or subcontractors will need to review the SF XXX to determine the information under the contract or subcontract that is considered CUI and how to properly safeguard the CUI. It is estimated that approximately 22,680 offerors, contractors, and subcontractors may review 2,092,918 forms for information on how to protect CUI each year. On average, it is estimated that it will take an offeror, contractor, or subcontractor two hours to review the SF XXX. The estimated annual cost to review standard forms is $334,866,880 (2,092,918 forms * 2 hours/form * $80), of which $5,058,880 is attributed to 15,809 small businesses.

c. Prepare and Distribute the SF XXX

If the contractor intends to flow down CUI to a subcontractor, then the contractor must prepare an SF XXX and distribute it to the subcontractor to ensure the subcontractor properly safeguards CUI. It is estimated 517,392 standard forms may be prepared and distributed by contractors and

[1] CISA OCE. (2020). *Cost of a Cyber Incident: Systematic Review and Cross-Validation. https://www.cisa.gov/sites/default/files/publications/CISA-OCE_Cost_of_Cyber_Incidents_Study-FINAL_508.pdf.*

subcontractors each year. On average, it is estimated that it will take the contractor or subcontractor two hours to prepare and distribute the SF XXX. The estimated annual cost to prepare and distribute the SF XXX is $82,782,270 (517,392 forms * 2 hours/form * $80), of which $2,529,440 is attributed to 15,809 small business contractors and subcontractors.

d. Train Employees on Handling CUI

A contractor shall not permit any contractor employee to collect, develop, receive, transmit, use, handle, or store CUI unless the employee has completed training on properly handling CUI as described in the SF XXX. The contractor must provide evidence of employee training upon request by the contracting officer; however, such requests are expected to be limited to, for example, instances in which the Government is dealing with a CUI incident. It is estimated that approximately 2,191,400 contractor and subcontractor employees may be required to take training on handling CUI, which is expected to take one hour to complete. It is anticipated that agencies will provide their support contractors and personnel with CUI standard training aligned with Federal policy.

The estimated annual training cost is $166,546,400 (2,191,400 employees * 1 hour/employee * $76/hour), of which $26,440,400 is attributed to 34,790 small business contractors and subcontractors. The estimated annual recordkeeping cost to maintain contractor training records is $10,003,741 (2,191,400 records * 0.083 hours/record * $55/hour), of which $1,588,164 is attributed to the 34,790 small businesses. The estimated annual reporting cost is $19,664 (1,430 requests * 0.25 hours/response * $55/hour), of which $13,401 is attributed to 975 small businesses.

e. Comply With NIST SP 800–172

A limited number of contractors may be required to implement NIST SP 800–172, Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800–171, for components of non-Federal systems that process, store, or transmit CUI or that provide security protection for such components when the designated CUI is associated with a critical program or high-value assets. Contractors that are subject to these enhanced security requirements may incur additional process/information technology configuration, network isolation, and security operations center/threat-related costs; however, the impact on any particular contractor may vary considerably, depending on a contractor's current infrastructure and development environment, and the composition of their customer base.

It is estimated that approximately 160 contractors may be subject to the enhanced security requirements. Of these 160 contractors, 100 are categorized as small businesses with 25–50 end-point systems. The estimated cost of initial implementation of NIST SP 800–172 for each of these contractors is $202,500. Twenty contractors are estimated to have 50–100 end-point systems (medium businesses) and 40 are expected to have 750–1500 end-point systems (large businesses). The estimated costs of initial implementation for these contractors are approximately $1,000,000 per medium business and $2,315,000 per large business.

Therefore, the total estimated cost for 160 contractors to implement NIST SP 800–172 is $132,850,000, of which $20,250,000 is attributed to 100 small businesses. Annual recurring costs are estimated to be 20 percent of the cost of initial implementation.

f. Submit Supporting Documentation To Verify Compliance

A contractor may also be required to submit to the Government a description of the system security plan required by NIST SP 800–171 Revision 2 to demonstrate their implementation of the security requirements in NIST SP 800–171 Revision 2. Requests for access to review the system security plan are expected to be rare, such as in response to a reported CUI incident. It is estimated that the system security plan may be requested 1,430 times and that it would take a contractor 30 minutes to submit the plan. The total estimated annual cost is $67,925 (1 request * 1,430 contractors * 0.5 hours/response * $95/hour), of which $46,294 is attributed to 975 small businesses.

Note, the cost to develop and maintain a system security plan in accordance with NIST SP 800–171 Revision 2 is attributed only to non-defense contractors (see sections IV.C.2.a. and IV.C.2.d. of this preamble) since defense contractors are subject to NIST SP 800–171 Revision 2 pursuant to DFARS clause 252.204–7012 and should already maintain system security plans.

g. Comply With Additional Security Requirements Identified in the Solicitation or Requirements Document

In addition to the security requirements outlined in the SF XXX and the new FAR clause at 52.204–XX, the requirements document may require the contractor to comply with controls beyond NIST SP 800–171 Revision 2 to address unique requirements to protect CUI Basic at higher than the moderate confidentiality level in accordance with 32 CFR 2002.14(h)(2). Similarly, if offerors require access to CUI, the Government will provide agency procedures on handling the CUI to ensure compliance with the requirements in 32 CFR 2002. The contractor shall also implement additional information security requirements it reasonably determines necessary to provide adequate security in a dynamic environment. Given that agencies have discretion in developing their contract-specific requirements, the Government does not attempt to quantify these costs.

h. Comply With Additional Notification and Marking Requirements

Offerors and contractors are required to notify the contracting officer representative or other designated agency official concerning any unmarked or mismarked CUI if discovered. These potential costs are not quantified since such occurrences are expected to be rare. In addition, to the maximum extent practicable, the offeror or contractor shall identify and mark its proprietary business and attributional information. These costs are also not quantified since an offeror or contractor usually marks its proprietary information as a best business practice to protect its own interests and information. Finally, offerors are required to notify the contracting officer of a potential CUI incident within 8 hours of discovery. Such occurrences are expected to be rare and are assumed to be accounted for under the public cost estimate for CUI incident reporting in section IV.C.2.b. of this preamble.

2. Non-Defense Contractors and Subcontractors

a. Comply With NIST SP 800–171 Revision 2

A contractor may need to depend on the expertise of information security specialists to develop and document processes and procedures associated with each security requirement, perform the periodic scans, tests, and assessments necessary for some of the security requirements, and analyze the results. The amount of time necessary to perform the various tasks will vary by contractor depending on the number of employees and the complexity of its information systems. Some contractors may already have personnel performing some of the functions as a matter of good business practice to protect their

networks, while others may be starting with no in-house expertise.

The total estimated labor cost for a small business in the initial year is approximately $148,200 (average of 1,560 hours * $95), with a recurring annual labor cost of approximately $98,800 (1,040 hours * $95). The total estimated labor cost for a business other than a small business in the initial year is approximately $543,400 (average of 5,720 hours * $95), with a recurring annual labor cost of approximately $494,000 (5,200 hours * $95). Note, this does not include the time expected to maintain the system security plan (see section IV.C.2.d. of this preamble).

Businesses may also need to install software and/or hardware to implement NIST SP 800–171 Revision 2. Similar to the labor costs, the cost of the specific software or hardware varies based on the solution selected by the business, a decision that will take into consideration the number of users, the types of devices used, and the complexity of the network, among other things. The Government estimates that a small business, on average, may spend $27,500 on hardware and software during initial implementation and $5,000 annually thereafter to maintain compliance. On average, a business other than a small business may spend $140,000 on hardware and software in the initial year and $80,000 annually thereafter.

Therefore, the total estimated cost of labor, hardware, and software for 5,875 contractors to implement NIST SP 800–171 Revision 2 in the initial year is $1,524,706,500, of which $861,808,500 is attributed to 4,905 small businesses. The total estimated annual recurring maintenance costs are $1,065,919,000, of which $509,139,000 is attributed to 4,905 small businesses.

b. Assess and Report Suspected CUI Incidents

When the contractor discovers a suspected CUI incident, the contractor is required by the clause at FAR 52.204–XX and, when applicable, the clause at FAR 52.204–YY to: determine what CUI was or could have been improperly accessed, used, processed, stored, maintained, disseminated, disclosed, or disposed of; construct a timeline of user activity; and determine methods and techniques used to access CUI. The contractor shall report any suspected or confirmed CUI incident to the agency website or point of contact identified in the SF XXX, within 8 hours of discovery. The clause at FAR 52.204–XX also requires the contractor to include in the report as many of the applicable data elements located on the DIBNet website (*https://dibnet.dod.mil*) as are available and provide any remaining applicable data elements as soon as they become available. Subcontractors are required by FAR 52.204–XX(h) to notify the prime or next higher tier subcontractor within the same timeframe. When applicable, the clause at FAR 52.204–YY requires contractors to follow agency requirements related to the incident if it turns out CUI is involved.

It is estimated that there may be 580 incident reports submitted each year and that it may take a contractor four hours to prepare and submit CUI incident reports to civilian agencies. The total estimated annual cost for CUI incident reporting for non-defense contractors is $275,500 (580 non-defense contractors * 1 incident/non-defense contractor * 4 hours/response * $95/hour), of which $188,482 is attributed to 397 small businesses.

c. Preserve and Protect Images for Suspected CUI Incidents and Submit Media and Data for Damage Assessments

If a suspected or confirmed CUI incident has occurred on an information system, the contractor is required by the clause at FAR 52.204–XX to preserve and protect images of all known affected information systems and all relevant monitoring and packet capture data for at least 90 days from the submission of the report to allow the Government to request the media and data or decline interest during this 90 day period, after which, if no request has been made, the images need no longer be preserved.

It is estimated that it will take a contractor approximately 7.5 hours to preserve and protect images of all known affected information systems and all relevant monitoring and packet capture data, assuming 30 minutes to image, 2 hours to preserve monitoring and packet capture data, and 5 hours to upload images and set up storage space. The estimated annual cost to preserve and protect images associated with 580 CUI incidents is $413,250 (580 contractors * 1 recordkeeper/contractor * 7.5 hours/record * $95/hour), of which $282,722 is attributed to 397 small businesses. The estimated annual cost to submit media and data is $11,400 (48 non-defense contractors * 1 incident/non-defense contractor * 2.5 hours/response * 95/hour), of which $7,799 is attributed to 33 small businesses.

d. Maintain the System Security Plan

It is assumed that each of 10,242 non-defense contractors required to implement NIST SP 800–171 Revision 2 has one information security analyst who spends one hour per month (or 12 hours per year) maintaining the system security plan. The estimated annual recordkeeping cost is $11,675,880 (10,242 contractors * 1 record/recordkeeper * 12 hours/record * $95/hour), of which $7,987,980 is attributed to 7,007 small businesses.

e. Cooperate With Validation Actions for Non-Federal Information Systems

The contractor shall cooperate with validation actions conducted by an agency in accordance with NIST SP 800–171A, Assessing Security Requirements for Controlled Unclassified Information, and if applicable, NIST SP 800–172A for the enhanced security requirements. These types of validation actions are similar to the High Confidence Level Assessments being conducted by DoD pursuant to DFARS clause 252.204–7020, NIST SP 800–171 DoD Assessment Requirements, whereby the Government reviews the system security plan description of how each security requirement is met and the contractor demonstrates its implementation. While cooperating with validation actions, a contractor may need to provide the Government access to its facilities, systems, and personnel.

According to DoD, the total estimated cost for a contractor to participate in a strategic High Confidence Level Assessment is approximately $50,675 per contractor. Therefore, the total annual estimated cost for the 110 non-defense contractors to cooperate with Government validation of a system security plan is $5,574,250, of which $4,104,675 is attributed to 81 small businesses.

f. Comply With NIST SP 800–53 and the FedRAMP Moderate Baseline Standards

The costs associated with contractor compliance with NIST SP 800–53 and the FedRAMP Moderate baseline standard for cloud service providers are excluded from this analysis of public cost, as they are being addressed under the proposed rule implementing section 2.i. of Executive Order 14028, Improving the Nation's Cyber Security (reference FAR Case 2021–019, Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems).

D. Government Costs

The total estimated Government costs associated with this FAR rule in billions over a ten-year period are as follows:

Government cost	Undiscounted	2 Percent
Present Value	$4.69	$4.21
Annualized	0.47	0.47

Undiscounted Government costs (in billions) by year over the ten-year period are summarized as follows:

Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Year 8	Year 9	Year 10
0.47	$0.47	$0.47	$0.47	$0.47	$0.47	$0.47	$0.47	$0.47	$0.47

The following is a summary from the RIA of the Government costs associated with reviewing contractor training records, investigating reports of suspected or confirmed CUI incidents, and other action associated with this FAR rule.

1. Prepare the SF XXX

While an SF XXX is required to be included in every solicitation and contract that involves CUI, except those exclusively for COTS items, the Government only incurs a significant cost when the CUI is identified on the form. The contracting officer is responsible for ensuring that the SF XXX identifies the protected information involved in the system of records and includes any safeguarding and marking requirements applicable to the information in accordance with FAR 4.403. Of the 2,092,918 forms expected to specify requirements for safeguarding CUI (see section IV.C.1.b. of this preamble), 1,573,582 are expected to be prepared by the Government (see section IV.C.1.c. of this preamble for the estimate of forms prepared by contractors and subcontractors). The total estimated annual Government cost is $453,191,616 (1,573,582 forms * 4 hour/form * $72/hour).

2. Review Training Records

It is estimated that it will take a Government employee 30 minutes to review evidence of training submitted by the contractors (see section IV.C.1.d. of this preamble). Therefore, the estimated annual reporting cost is $51,480 (1,430 requests * 0.5 hours/response * $72/hour).

3. Review CUI Incident Reports

It is estimated that it will take a Government employee four hours to review the CUI incident information reported by a contractor (see section IV.C.2.b. of this preamble). The estimated annual cost to the Government is $292,900 (580 reports * 5 hours/response * $101/hour).

4. Review Media and Data for Damage Assessment

It is estimated that it will take a Government employee 10 hours to conduct a damage assessment of media and data submitted by a contractor (see section IV.C.2.c. of this preamble). The estimated annual cost to the Government is $48,480 (48 submissions * 10 hours/response * $101/hour).

5. Review System Security Plan

It is estimated that it will take a Government employee four hours to review a system security plan submitted by a contractor (see section IV.C.1.g. of this preamble). The estimated annual cost to the Government is $577,720 (1,430 reports * 4 hours/response * $101/hour).

6. Conduct Validation Actions for Non-Federal Information Systems

For the purposes of this analysis, it is assumed that the cost to a civilian agency to validate a contractor's system security plan (see section IV.C.2.e. of this preamble) will be similar to the cost for DoD to perform a strategic High Confidence Level Assessment, approximately $51,097 per action. Therefore, the total annual estimated cost for civilian agencies to perform these validations is $5,620,670 (110 non-defense contractor system security plan reviews * $51,097/review).

7. Training Government Employees on New Requirements for CUI

It is expected that the Government contracting officers, contract specialists, contracting officer representatives, and others involved in the acquisition process, such as program managers and those involved in the development of requirements documents, will be required to become familiar with the technical requirements of this rule and receive additional training. While the requirement to remain current on policies for Government procurement, such as changes to the FAR, is considered a part of the normal duties of such individuals, there is expected to be specialized Government training on this topic, the cost of which is attributed to this rule. It is estimated that 250,000 Government employees may need to take 30 minutes of specialized training at an average wage rate equivalent to a GS–12, step 5, Government employee. Therefore, the estimated annual training cost is $9,000,000 (250,000 employees * 0.5 hours/employee * $72/hour).

E. Total Costs

The total estimated costs (in billions) associated with this FAR rule over a ten-year period are as follows:

Government Cost	Undiscounted	2 percent
Present Value	$22.32	$20.10
Annualized	2.23	2.24

Undiscounted public and Government costs (in billions) by year over the ten-year period are summarized in the following table:

Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Year 8	Year 9	Year 10
$2.75	$2.17	$2.17	$2.17	$2.17	$2.17	$2.17	$2.17	$2.17	$2.17

F. Alternatives Considered

1. Status Quo

Absent this FAR rule, agencies will continue to employ ad hoc, agency-specific policies to manage CUI. This approach can cause agencies to mark and handle this information inconsistently and inefficiently, and forces defense and non-defense contractors to establish procedures and internal controls to meet different civilian and defense agency approaches for marking and handling CUI. This approach was determined to be counter to the purpose of the Federal Acquisition Regulations System, which was established for the codification and publication of uniform policies and procedures for acquisition by all executive agencies (see FAR 1.101).

2. No Standard Form

The Government considered whether or not to establish a new standard form to communicate CUI requirements specific to the contract. As an alternative, the FAR could prescribe only a solicitation provision and contract clause to establish offeror and contractor responsibilities related to marking and handling CUI involved in the contract but would not dictate how agencies communicate what types of CUI may be involved in the contract. Given the importance of protecting CUI, it was determined that a Standard Form is the best way to ensure the Government is properly communicating specific CUI requirements for each contract. Absent a standard form, there is a risk that agencies may not provide enough information for contractors to understand what CUI is involved in the contract and what responsibilities they have with regard to this CUI. The standard form also provides a means for contractors to uniformly communicate CUI requirements to its subcontractors.

3. 100 Percent Inspection

Several aspects of this proposed rule require the contractor to provide information upon request. For example, contractors may be requested to submit supporting documentation to verify compliance with the system security plan required by NIST SP 800–171 Revision 2 in instances where the Government is dealing with a CUI incident that is a confirmed breach or an agency determines that it is necessary to verify a contractor's system security plan based on the criticality of a program and the CUI being handled on the contractor's information system (see sections B.1.e. and D.1.g. of the Regulatory Impact Analysis). Similarly, when such CUI incidents have occurred, the Government may require the contractor to submit information to verify that the contractor and its subcontractors have provided appropriate training to their employees that handle CUI, as required by the clause at FAR 52.204–XX (see sections B.1.c. and D.1.b of the Regulatory Impact Analysis).

As an alternative, the Government considered whether to require contractors to submit evidence of its system security plan and evidence that employees have been trained on an annual basis. However, defense contractors should have already implemented system security plans in accordance with DFARS clause 252.204–7012 and non-defense contractors have incentive to ensure compliance with the requirements in FAR clause 52.204–XX to avoid liability for breaches of CUI that may result from improperly protecting CUI being handled on the contractor's information system. As such, implementing a 100 percent inspection requirement would unnecessarily and significantly increase the burden on contractors and the Government.

4. Implementation of NIST SP 800–171 Revision 3

This proposed rule requires contractors to implement the requirements of NIST SP 800–171 Revision 2. In May of 2024, NIST published Revision 3 to NIST SP 800–171 (see *https://csrc.nist.gov/pubs/sp/800/171/r3/final*). The Government is currently assessing where the organizationally-defined parameters within Revision 3 should be standardized and implemented on a governmentwide basis. As stated in the benefits section of this rule, it is important for the Government to immediately implement requirements to protect CUI on non-Federal information systems; therefore, this proposed rule does not seek to implement NIST's most recent revision. The FAR Council anticipates that future rulemaking will be initiated to update NIST SP 800–171 and NIST SP 800–171A to the current version.

V. Specific Questions for Public Comment

To understand the exact scope of this impact and how this impact could be affected in the final rule, DoD, GSA, and NASA welcome input on the following questions regarding anticipated impact on affected parties. DoD, GSA, and NASA recognize that some agencies may need to tailor the approach to the information collected based on the unique mission and risks for their agency.

1. Is there additional information or guidance you view as necessary to effectively comply with this rule?

2. Are there specific situations you anticipate where your organization will be required to report on different timelines in order to comply with the CUI incident reporting requirements outlined in this proposed rule, other Federal contract requirements, or other regulations promulgated under Federal law? How would your organization handle disparate incident reporting timelines in other Federal Government contracting requirements or from other regulatory agencies?

3. Incident response and associated reporting are often iterative processes, with system owners updating reports as a situation evolves and more data becomes available. What implications are there for your organization, including with respect to incident response, to meet disparate timelines for incident reporting?

4. How much, if at all, would you estimate that the initial reporting requirement described in this proposed rule could increase the price of the products or services your organization provides to the Federal Government?

5. Understanding evolving data capabilities may change the nature or sensitivity of information over time, are there specific concerns not adequately addressed in this proposed rule? If possible, please provide any relevant use cases.

6. The FAR Council notes there is also what is referred to as ''CUI specified'', which is information that is considered CUI, but is also required to be handled in a certain way due to other laws, regulations, and policies (*e.g.,* restrictions on disseminating information to foreign nationals or dual citizens under International Traffic in Arms Regulations (ITAR)). For CUI specified information, not only does it have to be treated and handled as CUI,

but it also must be handled in accordance with the other applicable regulations and laws. Are there specific concerns not addressed in this proposed rule in this area? If so, please provide a relevant use case.

VI. Executive Orders 12866 and 13563

Executive Orders (E.O.s) 12866 (as amended by E.O. 14094) and 13563 direct agencies to assess the costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). E.O. 13563 emphasizes the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. This is a significant regulatory action and, therefore, was subject to review under section 6(b) of E.O. 12866, Regulatory Planning and Review, dated September 30, 1993.

VII. Regulatory Flexibility Act

DoD, GSA, and NASA expect this proposed rule, if finalized, to have a significant economic impact on a substantial number of small entities within the meaning of the Regulatory Flexibility Act, 5 U.S.C. 601–612. The Initial Regulatory Flexibility Analysis (IRFA) is summarized as follows:

DoD, GSA, and NASA are proposing to revise the FAR to implement a NARA final rule on the Federal CUI Program as it relates to performance under Federal contracts (see 32 CFR part 2002).

This proposed rule creates two new clauses at FAR 52.204–XX, Controlled Unclassified Information, and FAR 52.204–YY, Identifying and Reporting Information That Is Potentially Controlled Unclassified Information, and a new FAR provision at 52.204–WW, Notice of Controlled Unclassified Information Requirements. These clauses and the provision work together to implement a uniform way for Federal agencies, offerors, and contractors to manage CUI. The rule also creates a new standard form (SF) XXX to standardize the way in which the Government identifies CUI that will be managed and safeguarded by a contractor in performance of a contract. This rule is just one element of a larger strategy to improve the Government's efforts to identify, deter, protect against, detect, and respond to increasingly sophisticated attacks by criminals and our adversaries targeting Federal information and information systems.

Promulgation of this FAR rule is authorized by 41 U.S.C. 1121(b); 41 U.S.C. 1303; 40 U.S.C. 121(c); 10 U.S.C. chapter 4 and 10 U.S.C. chapter 137 legacy provisions (see 10 U.S.C. 3016); and 51 U.S.C. 20113.

This rule will apply to small businesses that are awarded Government contracts, other than those that receive awards exclusively for COTS items. According to award data in the Federal Procurement Data System (FPDS) for fiscal years (FY) 2021 through FY 2023, on average per year the Government awards contracts and orders for supplies and services (excluding those for supplies purchased using commercial item procedures) to 67,547 unique contractors, of which 44,152 (65 percent) are small businesses.

When an SF XXX is incorporated in the contract and identifies CUI that will be involved in the contract, the contractor will be subject to the new FAR clause at FAR 52.204–XX and more robust compliance requirements for safeguarding the CUI. Per the FPDS data, of the contractors that receive covered awards each year, approximately 37,933 are non-defense contractors and 29,614 are defense contractors, or contractors that do business with both civilian agencies and DoD. Based on consultation with subject matter experts, it is assumed that 18 percent of non-defense contractors (6,828) and 28 percent of defense contractors (8,292), or 15,120 total contractors, may receive awards each year that include an SF XXX listing CUI and the associated safeguarding requirements. It is further assumed that the ratio of subcontractors to prime contractors that handle CUI is 0.5:1, or 7,560 total subcontractors.

Therefore, each year, an estimated 22,680 contractors and subcontractors, of which 15,809 (70 percent) are estimated to be small businesses, will be required to safeguard CUI in performance of a contract, pursuant to the new clause at FAR 52.204–XX and the instructions provided on an SF XXX. These small entities may be impacted by the various compliance requirements in the clause, depending on the type of CUI required to be handled under the contract or subcontract, the way in which the information will be handled, and whether those small businesses have already been safeguarding sensitive Government information under other contract provisions.

The new FAR clause at 52.204–XX is modeled after the existing clause at DFARS 252.204–7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, the most recent version of which has been in effect since 2017 (the clause has been in effect since 2013, and the NIST SP 800–171 requirements were added in 2015). As such, small businesses that do business with DoD and handle CUI in performance of their contracts are already subject to requirements equivalent to the new FAR clause and provision. In addition, small businesses that do business with other agencies that have included similar or overlapping safeguarding requirements under agency-specific contract terms may already be in partial or substantial compliance with the clause requirements.

The following specific compliance requirements will apply to all Federal offerors, contractors, and subcontractors:

- *Review and Distribute the SF XXX.* When the contract includes an SF XXX that identifies CUI to be safeguarded under the contract, the contract will include the CUI clause. The contractor or subcontractor will need to review the SF XXX to determine what information under the contract is considered CUI and subject to the compliance requirements of the CUI clause. If the contractor or subcontractor intends to flow down CUI in performance of the contract or subcontract, then the contractor or subcontractor will need to prepare an SF XXX, as appropriate for CUI that will flow down, and distribute it to the subcontractor that will be handling CUI.
- *Train Contractor Employees on Handling CUI.* Per the CUI clause, a contractor shall not permit any contractor employee to have, retain access to, create, collect, use, process, store, maintain, disseminate, disclose, dispose of, or otherwise handle, CUI unless the employee has completed training on properly handling CUI that, at a minimum, includes the elements required in the SF XXX. The SF XXX will also specify the frequency at which a contractor must provide the training, which is dependent on the type of CUI being handled by the contractor's employees and the criticality of the program being supported. The contractor must provide evidence of employee training upon request by the contracting officer; however, such requests are expected to be limited to, for example, instances where the Government is dealing with a CUI incident, or where an agency determines that it is necessary to verify training based on the criticality of a program and the CUI being handled by the contractor.
- *Comply with NIST SP 800–172.* A limited number of contractors may be required under FAR clause 52.204–XX, Controlled Unclassified Information, to

implement some or all requirements of NIST SP 800–172, Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800–171, Revision 2. NIST SP 800–172 provides enhanced security requirements that apply only to components of nonfederal systems that process, store, or transmit CUI or that provide security protection for such components when the designated CUI is associated with a critical program or high-value asset. The enhanced requirements supplement the basic and derived security requirements in NIST Special Publication 800–171, Revision 2, and address the protection of CUI by promoting: penetration-resistant architecture, damage-limiting operations, and designs to achieve cyber resiliency and survivability.

• *Submit Supporting Documentation to Verify Compliance.* Per FAR clause 52.204–XX, Controlled Unclassified Information, upon request, a contractor shall submit the description of the system security plan required by NIST SP 800–171, Revision 2, (and NIST SP 800–172, when applicable) and any associated plans of action for any planned implementations or mitigations to the Government to demonstrate the contractor's implementation or planned implementation of the security requirements. Requests for the system security plan are expected to be rare or limited to, for example, instances where the Government is dealing with a CUI incident, or an agency determines that it is necessary to verify a contractor's system security plan based on the criticality of a program and the CUI being handled on the contractor's information system.

• *Comply with any additional security requirements identified in the Requirements Document.* In addition to the security requirements outlined in the SF XXX and the CUI clause, the requirements document in the contract may require the Contractor to comply with additional security requirements beyond NIST SP 800–171, Revision 2, to address unique requirements to protect CUI Basic at higher than the moderate confidentiality level in accordance with 32 CFR 2002.14(h)(2). The Contractor shall also implement additional information security requirements it reasonably determines necessary to provide adequate security in a dynamic environment.

• *Comply with Additional Notification Requirements.* Unmarked or mismarked CUI is not considered a CUI incident if the mismarking has not resulted in the mishandling or improper dissemination of the information. Per the new solicitation provision and contract clauses, offerors are requested and contractors are required to notify the Contracting Officer Representative or other designated agency official concerning any unmarked or mismarked CUI if discovered. Such occurrences are expected to be rare.

• *Comply with Additional Marking Requirements.* To the maximum extent practicable, offerors and contractors are required to identify and mark any proprietary business or contractor-attributional information.

The following compliance requirements are attributed only to non-defense contractors and subcontractors that handle CUI, since defense contractors are already required to comply with these requirements pursuant to DFARS clause 252.204–7012:

• *Comply with NIST SP 800–171, Revision 2.* If the Contractor is operating a non-Federal information system that processes, stores, or transmits CUI identified in the contract, the CUI clause requires the contractor to comply with the security requirements in NIST Special Publication 800–171, Revision 2, or as authorized by the Contracting Officer and any CUI specified requirements identified in the SF XXX. NIST SP 800–171 Revision 2 includes 110 security requirements for non-Federal information systems that can be grouped into the following 14 categories: access control, awareness and training, audit and accountability, configuration management, identification and authentication, incident response, maintenance, media protection, personnel security, physical protection, risk assessment, security assessment, system and communications protection, and system and information integrity. Specific information on the 110 individual security requirements and various templates are available on the NIST website at *https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final.* Federal contractors that handle covered Federal information (CFI), a much broader category than CUI, on their information systems are already required to have implemented 17 of the 110 security requirements, which are already included in the clause at FAR 52.204–21, Basic Safeguarding of Covered Contractor Information Systems. Such requirements are considered ''met'' by all impacted contractors, regardless of size. For the remaining 93 security requirements, a contractor may need to establish a process or procedure, configure existing information technology that the contractor already owns, or acquire additional software or hardware.

• *Assess and report suspected CUI incidents.* When the Contractor discovers a suspected CUI incident, the CUI clause requires the contractor to determine what CUI was or could have been improperly accessed, used, processed, stored, maintained, disseminated, disclosed, or disposed of; construct a timeline of user activity; and determine methods and techniques used to access CUI. The Contractor shall report any suspected or confirmed CUI incident to the agency website or point of contact identified in the SF XXX, within 8 hours of discovery. The report shall include as many of the applicable data elements located on the DIBNet website as are available and provide any remaining applicable data elements as soon as they become available. In addition, if the Contractor is a FedRAMP authorized (Joint Authorization Board or Agency) Cloud Service Provider, the Contractor shall also report to the points of contact specified in the FedRAMP incident reporting guidelines as documented in the Cloud Service Provider Incident Response Plan. The requirements of the CUI clause are flowed down to subcontracts at all tiers; subcontractors are required to notify the prime contractor or next higher-tier subcontractor within the same timeframes.

• *Preserve and protect images for suspected CUI incidents and submit media and data for damage assessments.* If a suspected or confirmed CUI incident has occurred on an information system, the CUI clause requires the Contractor shall preserve and protect images of all known affected information systems and all relevant monitoring and packet capture data for at least 90 days from the submission of the report to allow the Government to request the media and data or decline interest during this 90-day period, after which, if no request has been made, the images need no longer be preserved.

• *Cooperate with Validation Actions for Non-Federal Information Systems.* The CUI clause requires the Contractor to cooperate with validation actions conducted by an agency in accordance with NIST SP 800–171A, Assessing Security Requirements for Controlled Unclassified Information, and if applicable, NIST SP 800–172A for enhanced security requirements. These types of validation actions are similar to the DoD's Strategic High Confidence Level Assessments being conducted by DoD pursuant to the clause at DFARS 252.204–7020, and NIST SP 800–171 DoD Assessment Requirements, whereby the Government reviews the system security plan description of how

each security requirement is met and the contractor demonstrates its implementation. While cooperating with validation actions, a contractor may need to provide the Government access to its facilities, systems, and personnel.

• *Comply with NIST SP 800–53.* The CUI clause requires the Contractor, when it is operating an information system identified in the SF XXX as a Federal information system that processes, stores, or transmits CUI identified in the contract, to comply with agency-identified security controls from NIST Special Publication 800–53 and any CUI Specified requirements identified in the SF XXX. In addition, cloud service providers must meet security requirements established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate Baseline (*https://www.fedramp.gov/documents/*).

The total estimated cost of compliance for small businesses is $937,017,841 in the initial year of implementation and $564,187,237 in each subsequent year. The cost per entity is dependent on whether the small business is required to implement NIST SP 800–171 Revision 2 or NIST SP 800–172 on their information systems. For more information on the specific compliance requirements and the expected cost impact on contractors, see section IV.C. of this preamble. A Regulatory Impact Analysis that includes a detailed discussion and explanation about the assumptions and methodology used to estimate the cost of this regulatory action, including the specific impact and costs for small businesses, is available at *www.regulations.gov* (search for ''FAR Case 2017–016'' click ''Open Docket,'' and view ''Supporting Documents'').

This proposed rule does not duplicate, overlap, or conflict with any other Federal rules. This proposed rule implements the requirements of 32 CFR part 2002 to ensure uniform implementation of Federal contractor requirements for managing CUI.

While this rule is modeled after DFARS clause 252.204–7012, it does not conflict with the existing clause. It is expected that the DFARS clause will be amended in the future to address DoD-specific requirements that may be in addition to the FAR clause.

DoD, GSA, and NASA were unable to identify any alternatives that would reduce the burden on small entities and still meet the objectives of 32 CFR part 2002. It is not possible to establish different compliance standards that take into account the resources available to small entities or exempt small entities from the rule, or any part thereof, that does not increase the risk of CUI incidents. However, by implementing a more standardized set of requirements for contractor information systems and for CUI safeguarding across agencies, small businesses that engage in contracts involving sensitive Government information might find it easier and less costly to meet security requirements for such information under this rule, because the variation of system configurations and requirements will be significantly reduced. This, in turn, may make such businesses more competitive for future Government contracts.

The Regulatory Secretariat Division has submitted a copy of the IRFA to the Chief Counsel for Advocacy of the Small Business Administration. A copy of the IRFA may be obtained from the Regulatory Secretariat Division. DoD, GSA, and NASA invite comments from small business concerns and other interested parties on the expected impact of this proposed rule on small entities.

DoD, GSA, and NASA will also consider comments from small entities concerning the existing regulations in subparts affected by the rule in accordance with 5 U.S.C. 610. Interested parties must submit such comments separately and should cite 5 U.S.C. 610 (FAR Case 2017–016), in correspondence.

VIII. Paperwork Reduction Act

The Paperwork Reduction Act (44 U.S.C. 3501–3521) applies because the proposed rule contains information collection requirements. Accordingly, the Regulatory Secretariat Division has submitted a request for approval of a new information collection requirement concerning controlled unclassified information to the Office of Management and Budget.

A. Public Burden for This Collection of Information

1. *System Security Plan.* Public reporting burden for this collection of information is estimated to average 0.50 hour per response including the time to prepare and submit the plan.

The annual reporting burden is estimated as follows:

Respondents: 1,430.

Total annual responses: 1,430.

Total burden hours: 715.

This estimate is based on approximately one response per respondent.

The annual recordkeeping burden is estimated as follows:

Recordkeepers: 10,242.

Total annual records: 10,242.

Total recordkeeping burden hours: 122,904.

This estimate is based on one recordkeeper who spends one hour per month (or 12 hours per year) maintaining the system security plan.

2. *Preserve, Protect, and Submit Media and Data.* Public reporting burden for this collection of information is estimated to average 2.5 hours per response including the time to prepare and complete the submission.

The annual reporting burden is estimated as follows:

Respondents: 48.

Total annual responses: 48.

Total burden hours: 120.

This estimate is based on approximately one response per respondent.

The annual recordkeeping burden is estimated as follows:

Recordkeepers: 580.

Total annual records: 580.

Total recordkeeping burden hours: 4,350.

This estimate is based on one recordkeeper who spends 7.5 hours per year to preserve and protect images of all known affected information systems and all relevant monitoring and packet capture data, assuming 0.5 hours to image, 2 hours to preserve monitoring and packet capture data, and 5 hours to upload images and set up storage space.

3. *CUI Incident Reporting.* Public reporting burden for this collection of information is estimated to average 5 hours per response including the time to prepare and submit a CUI incident report.

The annual reporting burden is estimated as follows:

Respondents: 580.

Total annual responses: 580.

Total burden hours: 2,900.

This estimate is based on approximately one response per respondent.

4. *Training Records.* Public reporting burden for this collection of information is estimated to average 15 minutes (0.25 hour) per response including the time to prepare and submit the evidence of training.

The annual reporting burden is estimated as follows:

Respondents: 1,430.

Total annual responses: 1,430.

Total burden hours: 357.5.

This estimate is based on approximately one response per respondent.

The annual recordkeeping burden is estimated as follows:

Recordkeepers: 53,225.

Total annual records: 2,191,400.

Total recordkeeping burden hours: 181,886.

This estimate is based on one recordkeeper who spends 5 minutes (0.083 hours) per record maintaining the employee training certificates.

5. *Prepare and Distribute the SF XXX.* Public reporting burden for this collection of information is estimated to average 2 hours per response including the time to prepare and distribute the SF XXX.

The annual reporting burden is estimated as follows:

Respondents: 22,680.

Total annual responses: 517,392.

Total burden hours: 1,034,784.

B. Request for Comments Regarding Paperwork Burden

Submit comments on this collection of information no later than March 17, 2025 through *https://www.regulations.gov* and follow the instructions on the site. All items submitted must cite OMB Control No. 9000–XXXX, Controlled Unclassified Information. Comments submitted in response to this rule will be made publicly available and are subject to disclosure under the Freedom of Information Act. For this reason, please do not include in your comments information of a confidential nature, such as sensitive personal information or proprietary information, or any information that you would not want publicly disclosed unless you follow the instructions below for confidential comments. Summary information of the public comments received, including any specific comments, will be posted on *https://www.regulations.gov.*

All filers using the portal should use the name of the person or entity submitting comments as the name of their files, in accordance with the instructions below. Anyone submitting business confidential/proprietary information should clearly identify any business confidential/proprietary portion at the time of submission, file a statement justifying nondisclosure and referencing the specific legal authority claimed, and provide a non-confidential/non-proprietary version of the submission. Any business confidential information should be in an uploaded file that has a file name beginning with the characters ''BC.'' Any page containing business confidential information must be clearly marked ''BUSINESS CONFIDENTIAL/PROPRIETARY'' on the top of that page.

The corresponding non-confidential/non-proprietary version of those comments must be clearly marked ''PUBLIC.'' The file name of the non-confidential version should begin with the character ''P.'' The ''BC'' and ''P'' should be followed by the name of the person or entity submitting the comments or rebuttal comments. All filers should name their files using the name of the person or entity submitting the comments. Any submissions with file names that do not begin with a ''BC'' will be assumed to be public and will be made publicly available through *https://www.regulations.gov.*

To confirm receipt of your comment(s), please check *https://www.regulations.gov,* approximately two-to-three days after submission to verify posting. If there are difficulties submitting comments, contact the GSA Regulatory Secretariat Division at 202–501–4755 or *GSARegSec@gsa.gov.*

Public comments are particularly invited on:

- The necessity of this collection of information for the proper performance of the functions of Federal Government acquisitions, including whether the information will have practical utility;
- The accuracy of the estimate of the burden of this collection of information;
- Ways to enhance the quality, utility, and clarity of the information to be collected; and
- Ways to minimize the burden of the collection of information on respondents, including the use of automated collection techniques or other forms of information technology.

Requesters may obtain a copy of the supporting statement from the General Services Administration, Regulatory Secretariat Division by calling 202–501–4755 or emailing *GSARegSec@gsa.gov.* Please cite OMB Control Number 9000–XXXX, Controlled Unclassified Information, in all correspondence.

List of Subjects in 48 CFR Parts 1, 2, 3, 4, 5, 7, 9, 11, 12, 15, 27, 33, 42, 52, and 53

Government procurement.

William F. Clark,

Director, Office of Government-wide Acquisition Policy, Office of Acquisition Policy, Office of Government-wide Policy.

Therefore, DoD, GSA, and NASA propose amending 48 CFR parts 1, 2, 3, 4, 5, 7, 9, 11, 12, 15, 27, 33, 42, 52, and 53 as set forth below:

■ 1. The authority citation for 48 CFR Parts 1, 2, 3, 4, 5, 7, 9, 11, 12, 15, 27, 33, 42, 52, and 53 continues to read as follows:

Authority: 40 U.S.C. 121(c); 10 U.S.C. chapter 4 and 10 U.S.C. chapter 137 legacy provisions (see 10 U.S.C. 3016); and 51 U.S.C. 20113.

PART 1—FEDERAL ACQUISITION REGULATIONS SYSTEM

■ 2. In section 1.106 amend in the table following the introductory text, by adding in numerical order, entries for ''52.204–WW'' and ''52.204–XX'' to read as follows:

1.106 OMB approval under the Paperwork Reduction Act.

* * * * *

FAR segment	OMB control No.
* * * * *	
52.204–WW	9000–XXXX
52.204–XX	9000–0182 and 9000–XXXX
* * * * *	

* * * * *

PART 2—DEFINITIONS OF WORDS AND TERMS

■ 3. Amend section 2.101 by—

■ a. Adding in alphabetical order the definitions for ''Contractor-attributional information'', ''Controlled unclassified information (CUI)'', ''CUI incident'', ''CUI Registry'', ''Federal information system'', and ''Information system''; and

■ b. Removing the definition for ''Federally controlled information system''.

The additions read as follows:

2.101 Definitions.

* * * * *

Contractor-attributional information means information that identifies the contractor or its employees directly or identifies them indirectly by grouping information that can be traced back to the contractor (*e.g.,* program description or facility locations).

* * * * *

Controlled unclassified information (CUI) means information that the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Governmentwide policy requires or permits an agency to handle using safeguarding or dissemination controls. CUI does not include—

(1) Classified information;

(2) Covered Federal information (see 4.404–1);

(3) Information a contractor possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency (see 32 CFR 2002.4); or

(4) Federally-funded basic and applied research in science, technology, and engineering at colleges, universities, and laboratories in accordance with National Security Decision Directive 189.

* * * * *

CUI incident means suspected or confirmed improper access, use, disclosure, modification, or destruction of CUI, in any form or medium.

CUI Registry means the online repository for all information, guidance, policy, and requirements on handling CUI. Among other information, the CUI Registry identifies all approved CUI categories and subcategories, provides general descriptions for each, identifies the basis for controls, establishes markings, and includes guidance on handling procedures (see *https://www.archives.gov/cui*).

* * * * *

Federal information system means an information system (44 U.S.C. 3502(8)) used or operated by an agency, by a contractor of an agency, or by another organization on behalf of an agency.

* * * * *

Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. 3502(8)).

* * * * *

PART 3—IMPROPER BUSINESS PRACTICES AND PERSONAL CONFLICTS OF INTEREST

■ 4. Amend section 3.104–4 by—
■ a. Revising the section heading;
■ b. Removing paragraph (c);
■ c. Redesignating paragraph (b) as paragraph (c);
■ d. Adding a new paragraph (b);
■ e. Revising the newly redesignated paragraph (c);
■ f. Revising paragraph (d); and
■ g. Removing from paragraph (e)(1) the words ''A contractor'' and adding ''An offeror or contractor'' in its place.

The revisions and additions read as follows:

3.104–4 Disclosure, protection, and marking of contractor information.

* * * * *

(b)(1) The clause at 52.204–XX, Controlled Unclassified Information, directs offerors and contractors to indicate or otherwise identify any contractor bid or proposal information, contractor-attributional information, proprietary business information, and source selection information submitted to the Government. The contracting officer should consult with the contractor if the contracting officer is unsure whether information provided by the contractor falls into one of these categories.

(2) Individuals responsible for preparing material that may be source selection information as described at paragraph (10) of the ''source selection information'' definition in 2.101 must mark the cover page and each page that the individual believes contains source selection information with the legend ''Source Selection Information-See FAR 2.101 and 3.104.'' Although the information in paragraphs (1) through (9) of the definition in 2.101 is considered to be source selection information whether or not marked, all reasonable efforts must be made to mark such material with the same legend.

(c) Contractor bid or proposal information, contractor-attributional information, proprietary business information, and source selection information must be marked and protected from unauthorized disclosure in accordance with 4.403, 14.401, 15.207, applicable law, and regulations, including 32 CFR part 2002. If the offeror or contractor submits information that could be controlled unclassified information (*e.g.,* proprietary business information), the contracting officer shall determine whether the information must be marked and protected in accordance with applicable law, policy, guidance, and agency procedures. Individuals who are unsure how to handle such information should consult with agency officials as necessary.

(d) Except as provided in paragraph (d)(3) of this section, the contracting officer must promptly notify the offeror or contractor in writing if the contracting officer believes that contractor proprietary business information, contractor-attributional information, contractor bid or proposal information, or information marked in accordance with 52.215–1(e) has been inappropriately marked. Notification should occur upon discovery and may be made prior to award. The offeror or contractor that has affixed the marking must be given an opportunity to justify the marking.

(1) If the offeror or contractor agrees that the marking is not justified or does not respond within the time specified in the notice, the contracting officer may remove the marking and release the information.

(2) If, after reviewing the contractor's justification, the contracting officer determines that the marking is not justified, the contracting officer must notify the offeror or contractor in writing before releasing the information.

(3) For technical data marked as proprietary by an offeror or contractor, the contracting officer must follow the procedures in 27.404–5.

* * * * *

PART 4—ADMINISTRATIVE AND INFORMATION MATTERS

■ 5. Revise the heading of subpart 4.4 to read as follows:

Subpart 4.4—Safeguarding Information and Information Systems

■ 6. Add section 4.401 to read as follows:

4.401 Definition.

Information, as used in this subpart, means any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, electronic, or audiovisual forms (see Office of Management and Budget (OMB) Circular A–130).

4.402 [Redesignated as 4.402–1]

■ 7. Redesignate section 4.402 as section 4.402–1.
■ 8. Add section 4.402 to read as follows:

4.402 Classified information.

4.403 [Redesignated as 4.402–2].

■ 9. Redesignate section 4.403 as section 4.402–2.
■ 10. Amend the newly redesignated section 4.402–2 by—
■ a. Revising paragraphs (b)(2)(i) and (ii); and
■ b. Removing from paragraph (c)(1) the reference ''4.402(d)(1)'' and adding ''4.402–1(d)(1)'' in its place.

The revisions read as follows:

4.402–2 Responsibilities of contracting officers.

* * * * *

(b) * * *

(2) * * *

(i) An appropriate Security Requirements clause in the solicitation (see 4.402–3(a)); and

(ii) As appropriate, in solicitations and contracts when the contract may require access to classified information, a requirement for security safeguards in addition to those provided in the clause 52.204–2, Security Requirements for Classified Information.

* * * * *

■ 11. Add sections 4.402–3, and 4.403 through 4.403–7 to read as follows:

4.402–3 Contract clause.

(a) The contracting officer shall insert the clause at 52.204–2, Security Requirements for Classified Information, in solicitations and contracts when the contract may require access to classified information, unless the conditions specified in paragraph (d) of this section apply.

(b) If a cost contract (see 16.302) for research and development with an educational institution is contemplated, the contracting officer shall use the clause with its Alternate I.

(c) If a construction or architect-engineer contract under which employee identification is required for security reasons is contemplated, the contracting officer shall use the clause with its Alternate II.

(d) If the contracting agency is not covered by the NISP and has prescribed a clause and alternates that are substantially the same as those at 52.204–2, the contracting officer shall use the agency-prescribed clause as required by agency procedures.

4.403 Controlled unclassified information (CUI).

4.403–1 Definitions.

As used in section 4.403—

CUI Basic means the subset of CUI for which the authorizing law, regulation, or Governmentwide policy does not set out specific handling or dissemination controls. CUI Basic must be handled according to the uniform set of controls set forth in 32 CFR part 2002 and the CUI Registry.

CUI Categories means those types of information for which laws, regulations, or Governmentwide policies require or permit agencies to exercise safeguarding or dissemination controls, and which has been listed in the CUI Registry.

CUI Specified means the subset of CUI for which the authorizing law, regulation, or Governmentwide policy contains specific handling controls that it requires or permits agencies to use and that differ from those for CUI Basic. The CUI Registry indicates which laws, regulations, and Governmentwide policies include such specific requirements.

Handling means any use of CUI, including but not limited to collecting, developing, receiving, transmitting, storing, marking, safeguarding, transporting, disseminating, reusing, and disposing of the information.

Lawful Government purpose means any activity, mission, function, operation, or endeavor that the Government authorizes or recognizes as within the scope of its legal authorities or the legal authorities of non-executive branch entities such as State and local law enforcement.

Limited dissemination control means any control identified on the CUI Registry that agencies may use to limit or specify CUI dissemination.

On behalf of an agency means a contractor uses or operates an information system or maintains or collects information for the purpose of processing, storing, or transmitting Federal information, and those activities are not incidental to providing a service or product to the Government.

4.403–2 General.

(a) Executive Order 13556 of November 4, 2010, entitled ''Controlled Unclassified Information,'' establishes a program to standardize executive branch management of information that requires safeguarding or dissemination controls. The National Archives and Records Administration's (NARA) Information Security Oversight Office (ISOO) is the executive agent for the Controlled Unclassified Information Program.

(b) This section implements 32 CFR part 2002, Controlled Classified Information (CUI).

(c) Part 24, Protection of Privacy and Freedom of Information, contains additional policy and procedures for safeguarding records that are protected by the Privacy Act.

(d) Part 27, Patents, Data, and Copyrights, contains policy and procedures for safeguarding information in patent applications and patents.

4.403–3 Applicability.

(a) The requirements for safeguarding CUI in this section apply when an offeror or contractor is expected to handle CUI, including instances when CUI resides on or transits through contractor information systems or within contractor facilities.

(b) The CUI requirements in the clause at 52.204–XX, Controlled Unclassified Information, apply when CUI will be involved in the contract. The CUI requirements in the clause at 52.204–YY, Identifying and Reporting Information That Is Potentially Controlled Unclassified Information, apply when no CUI will be involved in the contract.

4.403–4 Policy.

(a) The requiring activity will identify any CUI in the standard form (SF) XXX, Controlled Unclassified Information (CUI) Requirements, which must be incorporated in the contract. Contractors are required to safeguard only the CUI that is identified in the SF XXX. However, see 52.204–XX(c)(2).

(b) Offerors and contractors are required to safeguard CUI pursuant to section 4.403–2. For CUI identified on an SF XXX that is incorporated into a contract, the contractor shall comply with the CUI requirements in the clause at 52.204–XX and on the form itself.

(c) Unmarked or mismarked CUI is not considered a CUI incident unless the mismarking or lack of marking has resulted in the mishandling or improper dissemination of the information. Offerors are requested, and contractors are required, to notify the Government within 8 hours of discovery if they discover during the solicitation phase or performance of a contract any information they suspect is CUI, but is not listed on an SF XXX or is not marked or properly marked as required by an SF XXX. Offerors and contractors are not responsible for identifying or marking unmarked or mismarked CUI that is not identified in the SF XXX.

(d) The Government shall protect against the improper use or release of information that includes contractor proprietary business information or contractor-attributional information to the extent required by law.

(e) Applicable CUI requirements can be waived by the Government in accordance with 32 CFR 2002.38.

4.403–5 Procedures.

(a) For each requirement, except those exclusively for the acquisition of commercially available off-the-shelf items, the contracting officer shall obtain from the requiring activity an SF XXX that—

(1) Identifies what CUI is involved in the contract;

(2) Specifies if and how the contractor is to mark CUI involved in the contract (*e.g.,* when the contractor is generating or developing the CUI, or when the purpose of the contract is to mark CUI); and

(3) Conforms to 11.002(i).

(b)(1) If the contracting officer has a reason to question the information on the SF XXX, the contracting officer shall request that the requiring activity verify that the SF XXX is accurate.

(2) If the requiring activity has marked the ''Yes'' box in Part A of SF XXX, the contracting officer shall incorporate the SF in the solicitation and contract and the clause at 52.204–XX, as prescribed at 4.403–7, to communicate requirements for safeguarding CUI during contract performance.

(3) If the requiring activity has marked the ''No'' box in Part A of SF XXX, the contracting officer shall include in the contract file a copy of the SF XXX and include in the solicitation and contract the clause at 52.204–YY, as prescribed at 4.403–7, to communicate requirements related to CUI should the contractor encounter suspected CUI during performance or the contract.

(c) If the requiring activity states that there should be controlled access to the contents of the SF XXX or the SF XXX is marked as CUI itself, contracting officers shall follow agency procedures

for safeguarding and disseminating the SF XXX.

(d) If the contracting officer is notified or otherwise discovers that there is, or potentially could be CUI involved in the contract and it was not properly identified on an SF XXX, the contracting officer shall coordinate with the requiring activity to determine if the information is CUI. If the agency determines that the information is CUI, then the agency shall take the following steps:

(1) If the agency wants the contractor to handle this kind of CUI during performance of the contract, the contracting officer shall—

(i) Coordinate with the requiring activity to have the SF XXX updated;

(ii) Modify the contract to incorporate the new SF XXX and, if CUI was not previously anticipated under the contract, to remove the clause at 52.204–YY and incorporate the clause at 52.204–XX;

(iii) Consider any request for equitable adjustment submitted by the contractor, as appropriate; and

(iv) Provide to the contractor marking instructions for the CUI.

(2) If the agency does not want the contractor to handle this kind of CUI, the contracting officer shall coordinate with the requiring activity to address the CUI (*e.g.,* retrieve the CUI) and shall convey such instructions to the contractor.

(e) Contracting officers shall also refer to 3.104–4 for procedures related to the disclosure, protection, and marking of contractor proprietary business information, contractor bid or proposal information, and source selection information submitted to the Government.

(f) The contracting officer shall follow agency procedures when providing any CUI to an offeror to ensure offeror compliance with the requirements in 32 CFR part 2002.

4.403–6 CUI incident reports.

(a) Agencies shall protect against the improper use or release of information that includes contractor proprietary business information or contractor-attributional information to the extent required by law. See paragraph (g)(9) of 52.204–XX, Controlled Unclassified Information, for details on how contracting officers may use or share this information.

(b) For CUI in a non-Federally-controlled facility—

(1) Designate the agency point of contact to whom the contractor reports a CUI incident in the SF XXX Part C, Section IV. When the SF XXX is not used in a contract, the point of contact is the contracting officer (see 52.204–YY(b)).

(2) The SF XXX will list any special incident reporting requirements for CUI Specified.

(3) Upon notification of a CUI incident, the contracting officer shall notify the requiring activity of the CUI incident as soon as practicable and in accordance with agency procedures. If the CUI incident occurs on an order against an indefinite delivery contract, the ordering agency contracting officer shall make the contracting officer for the indefinite delivery contract aware of the notification.

(c) When the contractor is required to provide information system images preserved under the requirements of paragraph (g)(4) of the clause at 52.204–XX or as directed by the contracting officer in response to contractor notification under paragraph (b)(2) of the clause at 52.204–YY, in accordance with agency procedures, the contracting officer shall provide instructions to the contractor for submitting the system images. The contractor is required to hold the system images for 90 days unless the Government declines interest.

(d)(1) The contracting officer shall not interpret a contractor's report of a CUI incident to mean that the contractor or a subcontractor at any tier failed to provide adequate safeguards for CUI or otherwise failed to meet the requirements of the clause at 52.204–XX, without further analysis by the agency.

(2) When a CUI incident is reported, the contracting officer shall consult with appropriate agency personnel (*e.g.,* program office or requiring activity) before taking any action under the contract related to the CUI incident. When the contract includes the clause at 52.204–XX, the contracting officer shall consider such CUI incidents in the context of an overall assessment of the contractor's compliance with the requirements of the clause at 52.204–XX.

(3) Unmarked or mismarked CUI is not considered a CUI incident unless the mismarking or lack of marking has resulted in the mishandling or improper dissemination of the information. The contracting officer shall consult with the appropriate agency personnel concerning any unmarked or mismarked CUI in accordance with agency procedures.

4.403–7 Solicitation provision and contract clauses.

(a) Insert the provision at 52.204–WW, Notice of Controlled Unclassified Information Requirements, in solicitations that contain the clause at 52.204–XX or the clause at 52.204–YY.

(b) Except for solicitations and contracts solely for the acquisition of COTS items, insert the clause at 52.204–XX, Controlled Unclassified Information, and include an SF XXX Controlled Unclassified Information (CUI) Requirements, in solicitations and contracts if the requiring activity has marked the ''Yes'' box in Part A of the SF XXX.

(c) Insert the clause at 52.204–YY, Identifying and Reporting Information That Is Potentially Controlled Unclassified Information, in solicitations and contracts if the requiring activity has marked the ''No'' box in Part A of SF XXX, excluding solicitations and contracts solely for the acquisition of COTS items.

■ 12. Revise section 4.404 and add sections 4.404–1 through 4.404–3 to read as follows:

4.404 Basic Safeguarding of Covered Contractor Information Systems.

4.404–1 Definitions.

As used in section 4.404—

Covered contractor information system means an information system owned or operated by a contractor on which the contractor processes, stores, or transmits covered Federal information.

Covered Federal information means information provided by or created for the Government, when that information is other than—

(1) Simple transactional information (such as that necessary to process payments);

(2) Information already publicly released (such as on public websites), or marked for public release, by the Government;

(3) Federally-funded basic and applied research in science, technology, and engineering at colleges, universities, and laboratories in accordance with National Security Decision Directive 189;

(4) Controlled unclassified information (CUI); or

(5) Classified information.

4.404–2 Applicability.

(a) This section applies to all acquisitions, including acquisitions of commercial services or commercial products other than commercially available off-the-shelf (COTS) items, when a contractor's information system may contain covered Federal information as part of performance on the contract.

(b) While covered Federal information is not required to be marked or identified by the Government, some

administrative markings (*e.g.,* draft, deliberative process, predecisional, not for public release) can indicate that the information is covered Federal information.

4.404–3 Contract clause.

Insert the clause at 52.204–21, Basic Safeguarding of Covered Contractor Information Systems, in solicitations and contracts excluding solicitations and contracts solely for the acquisition of—

(a) COTS items; or

(b) Federally-funded basic and applied research in science, technology, and engineering at colleges, universities, and laboratories in accordance with National Security Decision Directive 189 when the agency does not provide any covered Federal information to the contractor.

4.1301 [Amended]

■ 13. Amend section 4.1301 by—

■ a. Removing from paragraph (a) the phrases ''PUB Number 201'', and ''Federally-controlled information'' and adding the phrases ''201'' and ''Federal information'' in their places, respectively.

■ b. Removing from paragraph (b) the phrases ''PUB 201'', and ''Federally-controlled information'' and adding the phrases ''201'' and ''Federal information'' in their places, respectively.

4.1303 [Amended]

■ 14. Amend section 4.1303 by removing the words ''Federally-controlled information'' and adding ''Federal information'' in its place.

Subpart 4.19 [Removed and Reserved]

■ 15. Remove and reserve subpart 4.19.

PART 5—PUBLICIZING CONTRACT ACTIONS

5.202 [Amended]

■ 16. Amend section 5.202 in paragraph (a)(8) by removing the phrase ''proprietary information'' and adding ''controlled unclassified information (*e.g.,* general proprietary business information)'' in its place.

5.301 [Amended]

■ 17. Amend section 5.301 in paragraph (b)(1) by removing the phrase ''proprietary information'' and adding ''controlled unclassified information (*e.g.,* general proprietary business information)'' in its place.

PART 7—ACQUISITION PLANNING

■ 18. Amend section 7.103 by adding paragraph (z) to read as follows:

7.103 Agency-head responsibilities.

* * * * *

(z) Ensuring agency planners—(1) Comply with the requirements of Executive Order 13556 of November 4, 2010, as implemented at 32 CFR part 2002 and in agency procedures, for controlled unclassified information (CUI). This does not apply to acquisitions for commercially available off-the-shelf items or for Federally-funded basic and applied research in science, technology, and engineering at colleges, universities, and laboratories in accordance with National Security Decision Directive 189 when the agency does not provide any CUI to the contractor; and

(2) Identify all categories of CUI in proposed acquisitions and incorporate them and accompanying CUI standards in requirements planning and the SF XXX, Controlled Unclassified Information (CUI) Requirements, as appropriate (see 4.403–4, 11.002(i), and 39.105).

* * * * *

■ 19. Amend section 7.105 by—

■ a. Removing from paragraph (b)(18)(i) the phrase ''(see subpart 4.4)'' and adding ''(see 4.402)'' in its place;

■ b. Removing from paragraph (b)(18)(iii) the phrase ''Federally-controlled information'' and adding ''Federal information'' in its place;

■ c. Revising paragraph (b)(18)(iv); and

■ d. Adding paragraph (b)(18)(v).

The revision and addition read as follows:

7.105 Contents of written acquisition plans.

* * * * *

(b) * * *

(18) * * *

(iv) For acquisitions that may require covered Federal information to reside in or transit through contractor information systems, discuss compliance with 4.404.

(v) For acquisitions that may require a contractor to have access to, create, collect, use, process, store, maintain, disseminate, disclose, or dispose of CUI, discuss the security, marking, training, incident reporting, and other requirements (*e.g.,* destruction) applicable to CUI (see 4.403–5 and 4.403–6).

* * * * *

■ 20. Amend section 7.503 by revising paragraph (d)(11) to read as follows:

7.503 Policy.

* * * * *

(d) * * *

(11) Contractors working in any situation that permits or might permit them to gain access to controlled unclassified information (CUI). See 4.403.

* * * * *

PART 9—CONTRACTOR QUALIFICATIONS

9.505 [Amended]

■ 21. Amend section 9.505 by removing from paragraph (b)(1) the phrase ''Proprietary information'' and adding the phrase ''Contractor proprietary business information'' in its place.

■ 22. Amend section 9.505–4 by—

■ a. Removing from paragraph (a) introductory text the phrase ''proprietary information from others'' and adding ''another contractor's proprietary business information'' in its place; and

■ b. Revising paragraph (b).

The revision reads as follows:

9.505–4 Obtaining access to proprietary information.

* * * * *

(b) A contractor that gains access to another contractor's proprietary business information in performing advisory and assistance services for the Government must agree with the other company to protect its information from unauthorized use or disclosure for as long as it remains proprietary and refrain from using the information for any purpose other than that for which it was furnished. The contracting officer shall obtain copies of these agreements and ensure that they are properly executed.

* * * * *

9.508 [Amended]

■ 23. Amend section 9.508 by removing from paragraph (h) introductory text and paragraph (h)(1) the phrase ''proprietary information'' and adding ''contractor proprietary business information'' in their places, respectively.

* * * * *

PART 11—DESCRIBING AGENCY NEEDS

■ 24. Amend section 11.002 by adding paragraph (i) to read as follows:

11.002 Policy.

* * * * *

(i) When agencies acquire products and services subject to 32 CFR part 2002, Controlled Unclassified Information (CUI) (see 4.403), the SF XXX, Controlled Unclassified Information (CUI) Requirements, must be incorporated in the contract and must identify, at a minimum—

(1) The CUI the contractor will handle in performance of the contract;

(2) Any CUI access and dissemination requirements placed on the contractor during performance of the contract;

(3) Federal and non-Federal information systems the contractor will use to handle CUI in the performance of the contract;

(4) System security and privacy requirements for each information system, as appropriate, and any additional security and privacy measures required by the agency;

(5) Any instructions for handling CUI during performance of the contract;

(6) Any CUI training requirements the contractor must adhere to in order to comply with 32 CFR 2002.30; and

(7) Any CUI incident reporting instructions required by the agency, to include the agency website or single point of contact.

PART 12—ACQUISITION OF COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES

■ 25. Amend section 12.202 by adding paragraph (f) to read as follows:

12.202 Market research and description of agency need.

* * * * *

(f) Requirements documents for acquisitions involving controlled unclassified information (CUI) shall—

(1) Comply with 32 CFR part 2002; and

(2) Incorporate all applicable handling and compliance instructions included in the SF XXX, Controlled Unclassified Information (CUI) Requirements (see 4.403 and 11.002(i)).

■ 26. Amend section 12.301 by revising paragraph (d)(5) to read as follows:

12.301 Solicitation provisions and contract clauses for the acquisition of commercial products and commercial services.

* * * * *

(d) * * *

(5) Insert the clause at 52.204–21, Basic Safeguarding of Covered Contractor Information Systems, in solicitations and contracts (except solicitations and contracts solely for the acquisition of COTS items), as prescribed in 4.404–3.

* * * * *

PART 15—CONTRACTING BY NEGOTIATION

15.407–1 [Amended]

■ 27. Amend section 15.407–1 by removing from the introductory text of paragraph (f) the phrase ''improper disclosure.'' and adding ''improper disclosure such as requirements for controlled unclassified information or classified information.'' in its place.

■ 28. Amend section 15.604 by—

■ a. Removing from paragraph (a) introductory text the phrase ''proprietary information'' and adding ''contractor proprietary business information'' in its place; and

■ b. Revising paragraph (a)(7).

The revision reads as follows:

15.604 Agency points of contact.

* * * * *

(a) * * *

(7) Instructions for identifying and marking contractor proprietary business information so that it is protected and administrative markings conform to 15.609.

* * * * *

15.606–2 [Amended]

■ 29. Amend section 15.606–2 by removing from paragraph (a) introductory text the phrase ''the legend'' and adding ''the administrative marking'' in its place.

■ 30. Amend section 15.609 by—

■ a. Removing from paragraphs (a) and (b) the phrase ''the following legend'' and adding the phrase ''the following administrative marking'' in its place;

■ b. Revising paragraph (c);

■ c. Removing from paragraph (d) the phrase ''clearly mark'' and adding the phrase ''clearly administratively mark'' in its place;

■ d. Removing from paragraph (e) the phrase ''and privileged or confidential information to the Government'' and adding ''privileged or confidential information, or other controlled unclassified information'' in its place;

■ e. Revising paragraph (f); and

■ f. Removing from paragraphs (g), (h) introductory text and (h)(1) the term ''legend'' and adding ''administrative marking'' in its place.

The revisions read as follows:

15.609 Limited use of data.

* * * * *

(c) The agency point of contact shall return to the offeror any unsolicited proposal marked with an administrative marking different from that provided in paragraph (a) of this section. The return letter will state that the proposal cannot be considered because it is impracticable for the Government to comply with the administrative marking and that the agency will consider the proposal if it is resubmitted with the proper administrative marking.

* * * * *

(f) When an agency receives an unsolicited proposal without any restrictive administrative marking from an educational or nonprofit organization or institution, and an evaluation outside the Government is necessary, the agency point of contact shall—

(1) Attach a cover sheet clearly marked with the administrative marking in paragraph (d) of this section;

(2) Change the beginning of this administrative marking by deleting ''All Government personnel'' and adding ''All Government and non-Government personnel''; and

(3) Require any non-Government evaluator to agree in writing that data in the proposal will not be disclosed to others outside the Government.

* * * * *

PART 27—PATENTS, DATA AND COPYRIGHTS

■ 31. Revise the heading of section 27.203 to read as follows:

27.203 Security requirements for patent applications and other patent information.

* * * * *

■ 32. Redesignate sections 27.203–1 and 27.203–2 as sections 27.203–2 and 27.203–3, and adding a new section 27.203–1 to read as follows:

27.203–1 Security requirements for controlled unclassified information.

Contracts involving patent applications or other patent-related controlled unclassified information require safeguarding or dissemination controls that must be identified in the SF XXX, Controlled Unclassified Information (CUI) Requirements. See 4.403.

■ 33. Revise the heading of newly redesignated section 27.203–2 to read as follows:

27.203–2 Security requirements for classified information.

* * * * *

PART 33—PROTESTS, DISPUTES, AND APPEALS

■ 34. Amend section 33.104 by—

■ a. Revising paragraph (a)(2); and

■ b. Removing from paragraph (a)(5) introductory text the phrase ''development or commercial information'' and adding ''development, commercial information, or other controlled unclassified information'' in its place.

The revision reads as follows:

33.104 Protests to GAO.

* * * * *

(a) * * *

(2) Immediately after receipt of the GAO's written notice that a protest has been filed, the agency shall give notice of the protest to the contractor if the award has been made, or, if no award has been made, to all parties who appear to have a reasonable prospect of receiving award if the protest is denied.

The agency shall furnish copies of the protest submissions to such parties with instructions to—

(i) Communicate directly with the GAO; and

(ii) Provide copies of any such communication to the agency and to other participating parties when they become known. However, if the protester has identified controlled unclassified information and requests a protective order, then the contracting officer shall obtain a redacted version from the protester to furnish to other interested parties, if one has not already been provided.

* * * * *

PART 42—CONTRACT ADMINISTRATION AND AUDIT SERVICES

42.302 [Amended]

■ 35. Amend section 42.302 by removing from paragraph (a)(21) the phrase ''Subpart 4.4'' and adding ''4.402'' in its place.

PART 52—SOLICITATION PROVISIONS AND CONTRACT CLAUSES

■ 36. Amend section 52.204–2 by revising the section heading, the introductory text, the clause heading, and the date of the clause to read as follows:

52.204–2 Security Requirements for Classified Information.

As prescribed in 4.402–3(a), insert the following clause:

Security Requirements for Classified Information (DATE)

* * * * *

■ 37. Amend section 52.204–9 by—

■ a. Revising the date of the clause;

■ b. Removing from paragraph (a) the phrase ''(FIPS PUB) Number'' and adding ''(FIPS)'' in its place; and

■ c. Removing from paragraph (d) the phrase ''Federally-controlled information'' and adding ''Federal information'' in its place.

The revision reads as follows:

52.204–9 Personal Identity Verification of Contractor Personnel.

* * * * *

Personal Identity Verification of Contractor Personnel (DATE)

* * * * *

■ 38. Amend section 52.204–16 by—

■ a. Revising the date of the clause; and

■ b. Removing from paragraph (g) the phrase ''Security Requirements'' and adding ''Security Requirements for Classified Information'' in its place.

The revision reads as follows:

52.204–16 Commercial and Government Entity Code Reporting.

* * * * *

Commercial and Government Entity Code Reporting (DATE)

* * * * *

■ 39. Amend section 52.204–18 by—

■ a. Revising the date of the clause; and

■ b. Removing from paragraph (f) the phrase ''Security Requirements'' and adding ''Security Requirements for Classified Information'' in its place.

The revision reads as follows:

52.204–18 Commercial and Government Entity Code Maintenance.

* * * * *

Commercial and Government Entity Code Maintenance (DATE)

* * * * *

40. Amend section 52.204–21 by—

■ a. Revising the introductory text and date of the clause;

■ b. In paragraph (a):

■ i. Revising the definition of ''Covered contractor information system'';

■ ii. Adding in alphabetical order the definition for ''Covered Federal information'';

■ iii. Removing the definition for ''Federal contract information'';

■ iv. Revising the definition of ''Information'';

■ c. Removing from paragraph (b)(1)(vii) the phrase ''Federal Contract Information'' and adding ''covered Federal information'' in its place.

■ d. Removing from paragraph (b)(2) the phrase ''controlled unclassified information (CUI)'' and adding ''CUI'' in its place;

■ e. Adding paragraph (b)(3); and

■ f. Removing from paragraph (c) the phrase ''Federal contract information'' and adding ''covered Federal information'' in its place.

The revisions and additions read as follows:

52.204–21 Basic Safeguarding of Covered Contractor Information Systems.

As prescribed in 4.404–3, insert the following clause:

Basic Safeguarding of Covered Contractor Information Systems (DATE)

(a) * * *

Covered contractor information system means an information system owned or operated by a contractor on which the contractor processes, stores, or transmits covered Federal information.

Covered Federal information means information provided by or created for the Government when that information is other than—

(1) Simple transactional information (such as that necessary to process payments);

(2) Information already publicly released (such as on public websites), or marked for public release, by the Government;

(3) Federally-funded basic and applied research in science, technology, and engineering at colleges, universities, and laboratories in accordance with National Security Decision Directive 189;

(4) Controlled unclassified information (CUI); or

(5) Classified information.

Information means any communication or representation of knowledge such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, electronic, or audiovisual forms (OMB Circular A–130, Managing Information as a Strategic Resource).

* * * * *

(b) * * *

(3) *Identification of covered Federal information.* While covered Federal information is not required to be marked or identified by the Government, some administrative markings (*e.g.,* draft, deliberative process, predecisional, not for public release) can indicate that the information is covered Federal information. If the Contractor is not sure whether specific information is covered Federal information, the Contractor can request clarification from the Contracting Officer.

* * * * *

■ 41. Add sections 52.204–WW, 52.204–XX, and 52.204–YY to read as follows:

52.204–WW Notice of Controlled Unclassified Information Requirements.

As prescribed in 4.403–7(a), insert the following provision:

Notice of Controlled Unclassified Information Requirements (DATE)

(a) *Definitions.* As used in this provision, *contractor-attributional information, contractor bid or proposal information, controlled unclassified information (CUI), CUI incident,* and *handling* have the meaning provided in the clause 52.204–XX, Controlled Unclassified Information.

(b) *Government-provided information.*

(1) The Offeror shall not use Government-provided information for its own purposes, whether or not the information is marked as CUI, unless the information is in the public domain, or unless the information was lawfully made available to the Offeror by someone other than the Government.

(2) If Offerors require access to CUI, the Government will provide agency procedures on handling the CUI to ensure compliance with the requirements in 32 CFR part 2002. Offerors shall comply with these agency procedures when handling CUI.

(c) *Offeror-provided information.* The Offeror shall appropriately identify information the Offeror owns and provides to the Government, which is contractor bid or proposal information, contractor-attributional information, or Offeror proprietary business information. The Government will determine in accordance with agency procedures whether the information provided by the Offeror is CUI or entitled to other protections (*e.g.,* contractor-attributional information associated with a CUI incident).

(d) *Unmarked CUI or mismarked CUI.* The Offeror should notify the Contracting Officer within 8 hours of discovery if the Offeror discovers any CUI that is not marked, not properly marked, not identified on the SF XXX, or is involved in a suspected or confirmed CUI incident. The Offeror should take action to appropriately safeguard any information the Offeror believes is CUI that is not identified in the SF XXX or is not marked or properly marked as required in the SF XXX until a Contracting Officer makes a determination.

(End of provision)

52.204–XX Controlled Unclassified Information.

As prescribed in 4.403–7(b), insert the following clause:

Controlled Unclassified Information (DATE)

(a) *Identifying controlled unclassified information.* The SF XXX, Controlled Unclassified Information, that is incorporated into this contract identifies what controlled unclassified information (CUI) is involved in the contract. The Contractor is required to safeguard only the CUI that is identified in the SF XXX. However, see paragraph (c)(2) of this clause.

(b) *Definitions.* As used in this clause—

Adequate security means security protections commensurate with the risk of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information.

Contractor-attributional information means information that identifies the Contractor or its employees directly or identifies them indirectly by grouping information that can be traced back to the Contractor (*e.g.,* program description or facility locations).

Contractor bid or proposal information means any of the following information submitted to a Federal agency as part of or in connection with a bid or proposal to enter into a Federal agency procurement contract, if that information has not been previously made available to the public or disclosed publicly:

(1) Cost or pricing data as defined by 10 U.S.C. 3701(1), with respect to procurements subject to that section, and 41 U.S.C. 3501(a)(2), with respect to procurements subject to that section.

(2) Indirect costs and direct labor rates.

(3) Proprietary information about manufacturing processes, operations, or techniques marked by the Contractor in accordance with applicable law or regulation.

(4) Information marked by the Contractor as ''Contractor bid or proposal information'' in accordance with applicable law or regulation.

(5) Information marked in accordance with 52.215–1(e).

Controlled unclassified information (CUI) means information that the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Governmentwide policy requires or permits an agency to handle using safeguarding or dissemination controls. CUI does not include—

(1) Classified information;

(2) Covered Federal information;

(3) Information a Contractor possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency (see 32 CFR 2002.4); or

(4) Federally-funded basic and applied research in science, technology, and engineering at colleges, universities, and laboratories in accordance with National Security Decision Directive 189.

CUI Basic means the subset of CUI for which the authorizing law, regulation, or Governmentwide policy does not set out specific handling or dissemination controls. CUI Basic must be handled according to the uniform set of controls set forth in 32 CFR part 2002 and the CUI Registry.

CUI categories means those types of information for which laws, regulations, or Governmentwide policies require or permit agencies to exercise safeguarding or dissemination controls, and which has been listed in the CUI Registry.

CUI incident means improper access, use, disclosure, modification, or destruction of CUI, in any form or medium.

CUI Registry means the online repository for all information, guidance, policy, and requirements on handling CUI. Among other information, the CUI Registry identifies all approved CUI categories and subcategories, provides general descriptions for each, identifies the basis for controls, establishes markings, and includes guidance on handling procedures (see *https://archives.gov/cui*).

CUI Specified means the subset of CUI for which the authorizing law, regulation, or Governmentwide policy contains specific handling controls that it requires or permits agencies to use and that differ from those for CUI Basic. The CUI Registry indicates which laws, regulations, and Governmentwide policies include such specific requirements.

Federal information system means an information system (44 U.S.C. 3502(8)) used or operated by an agency, or by a contractor of an agency or by another organization, on behalf of an agency.

Handling means any use of CUI, including but not limited to collecting, developing, receiving, transmitting, storing, marking, safeguarding, transporting, disseminating, re-using, and disposing of the information.

Information means any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, electronic, or audiovisual forms (see Office of Management and Budget (OMB) Circular No. A–130, Managing Information as a Strategic Resource).

Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. 3502(8)).

Lawful Government purpose means any activity, mission, function, operation, or endeavor that the Government authorizes or recognizes as within the scope of its legal authorities or the legal authorities of non-executive branch entities such as state and local law enforcement.

Limited dissemination control means any control identified on the CUI Registry that agencies may use to limit or specify CUI dissemination.

On behalf of an agency means a Contractor uses or operates an information system or maintains or collects information for the purpose of processing, storing, or transmitting Federal information, and those activities

are not incidental to providing a service or product to the Government.

(c) *Identifying and reporting information the Contractor believes or has reason to know is potentially CUI.*

(1) The Contractor shall notify the Contracting Officer within 8 hours of discovery if—

(i) The Contractor discovers any information that the Contractor believes is CUI that is not identified in the SF XXX or is not marked or properly marked as required in the SF XXX; or

(ii) There is any inconsistency between this clause and an SF XXX incorporated into the contract.

(2) The Contractor shall take action to appropriately safeguard any information the Contractor believes is CUI that is not identified in the SF XXX or is not marked or properly marked as required in the SF XXX until a Contracting Officer makes a determination.

(3) If the Contractor discovers any information that the contractor believes is CUI that is not identified in the SF XXX that is involved in a suspected or confirmed CUI incident, the Contractor shall notify the Contracting Officer and comply with paragraph (g) of this clause.

(4) The Contractor is not entitled to use Government-provided information for its own purposes, whether or not the information is marked as CUI, unless the information is in the public domain, or unless the information was lawfully made available to the Contractor by someone other than the Government.

(5) The Contractor shall appropriately identify information the Contractor owns and provides to the Government (*e.g.,* contractor bid or proposal information, contractor-attributional information, or contractor proprietary business information). The Government will determine in accordance with agency procedures whether the information provided by the Contractor is CUI or entitled to other protections (*e.g.,* contractor-attributional information associated with a CUI incident).

(d) *Safeguarding CUI.*

(1) The Contractor shall safeguard CUI that the Government identifies in the SF XXX and ensure handling consistent with 32 CFR 2002.14.

(i) This includes CUI that the Government provides to the Contractor or CUI that the Contractor collects, develops, receives, transmits, uses, handles, or stores in performance of the contract.

(ii) For CUI located within a Federally-controlled facility, the Contractor shall follow agency CUI policies and shall ensure that any Contractor employees handling CUI within Federally-controlled facilities meet the prerequisites identified within Part B on the SF XXX for training and for access to CUI.

(iii) For CUI located within a non-Federally-controlled facility, the Contractor shall follow CUI policies and shall ensure that any Contractor employees handling CUI within the non-Federally-controlled facility comply with the requirements identified in Part C of the SF XXX.

(iv) Any applicable agency-specific policies for safeguarding or handling CUI will be identified in the SF XXX.

(v) When information is not identified as CUI, it may be covered Federal information requiring information system security controls in accordance with Federal Acquisition Regulation clause 52.204–21, Basic Safeguarding of Covered Contractor Information Systems.

(2) The Contractor shall permit access to CUI only as described in the SF XXX.

(3) Except for its own information, the Contractor is not responsible for identifying or marking unmarked or mismarked CUI unless doing so is specifically included in the SF XXX, such as when the Contractor generates or develops the CUI.

(4) No Contractor employee shall be permitted to have or retain access to, create, collect, use, process, store, maintain, disseminate, disclose, dispose of, or otherwise handle CUI unless the employee has completed training on properly handling CUI that, at a minimum, includes the elements required in the SF XXX.

(5) Contractors operating information systems that access, use, process, store, maintain, or transmit CUI identified in the contract, shall implement the following requirements:

(i) When the Contractor is operating an information system identified in the SF XXX as a Federal information system—

(A) The Contractor shall comply with agency-identified security requirements from the latest version of National Institute of Standards and Technology (NIST) Special Publication (SP) 800–53 and any CUI Specified requirements identified in the SF XXX; and

(B) If using cloud computing services, the Contractor shall comply with agency-identified security requirements, but at no less than the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline (*https://www.fedramp.gov/documents/*).

(ii) When the Contractor is operating a non-Federal information system, the Contractor shall—

(A) Comply with the security requirements of NIST SP 800–171 Revision 2, ''Protecting Controlled Unclassified Information in Non-Federal Information Systems and Organizations'' (available via the internet at *https://dx.doi.org/10.6028/NIST.SP.800-171*) or as authorized by the Contracting Officer. Additional controls other than NIST SP 800–171 Revision 2 may be specified in the contract's requirements document, in accordance with 32 CFR 2002.14(h)(2), to address unique requirements to protect CUI Basic at higher than the moderate confidentiality level;

(B) Comply with all additional security requirements for CUI Specified identified by the agency in the SF XXX;

(C) Implement additional information security requirements the Contractor reasonably determines necessary to provide adequate security in a dynamic environment;

(D) Comply with any requirements from NIST SP 800–172, Enhanced Security Requirements for Protecting Controlled Unclassified Information, identified by the agency. For any requirements in NIST SP 800–172 identified by the agency, the organizational defined parameters (ODP) provided in Attachment 1 of SF XXX shall be applied for applicable security requirements;

(E) Ensure that, if the Contractor uses a cloud service provider to store, process, or transmit any CUI identified in SF XXX—

(*1*) The cloud service provider meets security requirements established by the Government for the FedRAMP Moderate baseline (*https://www.fedramp.gov/documents/*); and

(*2*) The additional requirements in paragraphs (d)(5)(ii)(B) and (C), and (g) of this clause are met; and

(F) Submit the system security plan, and any associated plans of action required by NIST SP 800–171, Revision 2, for any planned implementations or mitigations to the Government upon request to demonstrate the Contractor's implementation or planned implementation of the security requirements.

(e) *Compliance.*

(1) The Contracting Officer may require the submission of supporting documentation to verify compliance with the contract's security requirements, or may require access to Contractor facilities or systems, as listed in SF XXX.

(2) For applicable non-Federal information systems, the agency may conduct validation actions in accordance with NIST SP 800–171A, Assessing Security Requirements for Controlled Unclassified Information and, if applicable, NIST SP 800–172A,

Assessing Enhanced Security Requirements for Controlled Unclassified Information.

(f) *Training.*

(1) *General CUI training.* All Contractor employees who will handle CUI shall complete general CUI training before doing so, and periodically complete refresher training thereafter, as described in the training sections at Section II of Part B and Section III of Part C of the SF XXX. The Contractor shall maintain documentation of employee training and shall provide it to the Contracting Officer upon request.

(2) *Additional training.*

Additional agency-specific training. Contractor employees shall also take any additional training described in the SF XXX sections on training. This additional training augments the general CUI training and may include specialized training for a particular category of CUI or for certain employees handling CUI in a specific situation, or other similar circumstances.

(g) *CUI incidents.*

(1) For CUI in a Federally-controlled facility, the Contractor shall report CUI incidents in accordance with agency policy.

(2) For CUI in a non-Federally-controlled facility, the Contractor shall report—

(i) Any suspected or confirmed CUI incident to the agency website or single point of contact identified in Part C, Section IV of the SF XXX; if there is no point of contact identified there the Contractor should contact the Contracting Officer for instructions;

(ii) Within 8 hours of discovery; and

(iii) As many of the applicable data elements located at *https://dibnet.dod.mil/portal/intranet/* as are available in the initial report and provide any remaining applicable data elements as soon as they become available.

(3) When the Contractor discovers a suspected or confirmed CUI incident, the Contractor shall—

(i) Determine and inventory what CUI was or could have been improperly accessed, created, collected, used, processed, stored, maintained, disseminated, disclosed, or disposed of;

(ii) Construct a timeline of user activity;

(iii) Determine methods and techniques used to access CUI; and

(iv) Cooperate and exchange information with agency officials, as determined necessary by the agency, in order to effectively report and manage a suspected or confirmed CUI incident.

(4) If the suspected or confirmed CUI incident has occurred on an information system, preserve and protect images of all known affected information systems and all relevant monitoring and packet capture data until the Government declines interest or 90 days from the date of the submission of the report passes without the Government requesting the media and data, whichever is sooner.

(5) Unmarked or mismarked CUI is not considered a CUI incident unless the mismarking or lack of marking has resulted in the mishandling or improper dissemination of the information.

(6) If the Contractor is a FedRAMP authorized (Joint Authorization Board or Agency) cloud service provider, the Contractor shall also report to the point(s) of contact specified in the FedRAMP incident reporting guidelines as documented in the Cloud Service Provider Incident Response Plan.

(7) The reporting requirements of this clause do not relieve the Contractor from the requirement to follow any applicable laws, regulations, or policies outside of this clause.

(8) If the Contractor is determined to be at fault for a CUI incident (*e.g.,* not safeguarding CUI in accordance with contract requirements), the Contractor may be financially liable for Government costs incurred in the course of the response and mitigation efforts in addition to any other damages at law or remedies available to the Government for noncompliance.

(9)(i) The Government will protect contractor bid or proposal information, contractor proprietary business information, and contractor-attributional information related to a CUI incident, against unauthorized use or release to the extent required by law.

(ii) The agency may release outside the Government contractor bid or proposal information, contractor proprietary business information, and contractor-attributional information that is not created by or for the Government, but that is related to a CUI incident—

(A) To entities with missions that may be affected by such information;

(B) To entities that may be called upon to assist in the diagnosis, detection, or mitigation of CUI incidents; or

(C) For national security purposes, including cyber situational awareness.

(iii) The Government may use and release contractor bid or proposal information, contractor proprietary business information, and contractor-attributional information, created by or for the Government and related to a CUI incident, outside of the Government for purposes and activities associated with responding to a CUI incident and for any other lawful Government purpose or activity.

(iv) In any authorized release, the Government will minimize the contractor proprietary business information and contractor-attributional information that it includes.

(10) An agency, at its sole discretion, may obtain assistance from Federal agencies or entities outside the Government, such as third-party firms to aid incident response activities.

(11) The SF XXX will list in Part C, Section IV incident reporting requirements that differ from or are in addition to those in this clause, such as requirements for CUI in a CUI Specified category.

(h) *Subcontracts.*

(1) Except for the acquisitions in paragraph (h)(2), in subcontracts at any tier, or other contractual instruments, for which performance involves CUI identified in the SF XXX, Controlled Unclassified Information (CUI) Requirements, the Contractor shall—

(i) Include this clause, including this paragraph (h), without alteration except to identify the parties;

(ii) Include the information in the SF XXX, Controlled Unclassified Information (CUI) Requirements, modified as required to address the CUI that applies to the subcontract; and

(iii) Require subcontractors to notify the prime Contractor or next higher tier subcontractor within 8 hours of discovery of a suspected or confirmed CUI incident.

(2) Paragraph (h)(1) of this clause does not apply to acquisitions exclusively for commercially available off-the-shelf items or Federally-funded basic and applied research in science, technology, and engineering at colleges, universities, and laboratories in accordance with National Security Decision Directive 189 when the Contractor does not provide any CUI to the subcontractor.

(End of clause)

52.204–YY Identifying and Reporting Information That Is Potentially Controlled Unclassified Information.

As prescribed in 4.403–7(c), insert the following clause:

Identifying and Reporting Information That is Potentially Controlled Unclassified Information (DATE)

(a) *Definitions.* As used in this clause—

Contractor-attributional information means information that identifies the Contractor or its employees directly or identifies them indirectly by grouping information that can be traced back to the Contractor (*e.g.,* program description or facility locations).

Contractor bid or proposal information means any of the following

information submitted to a Federal agency as part of or in connection with a bid or proposal to enter into a Federal agency procurement contract, if that information has not been previously made available to the public or disclosed publicly:

(1) Cost or pricing data as defined by 10 U.S.C. 3701(1), with respect to procurements subject to that section, and 41 U.S.C. 3501(a)(2), with respect to procurements subject to that section.

(2) Indirect costs and direct labor rates.

(3) Proprietary information about manufacturing processes, operations, or techniques marked by the Contractor in accordance with applicable law or regulation.

(4) Information marked by the Contractor as ''Contractor bid or proposal information'' in accordance with applicable law or regulation.

(5) Information marked in accordance with 52.215–1(e).

Controlled unclassified information (CUI) means information that the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Governmentwide policy requires or permits an agency to handle using safeguarding or dissemination controls. CUI does not include—

(1) Classified information;

(2) Covered Federal information;

(3) Information a Contractor possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency (see 32 CFR 2002.4); or

(4) Federally-funded basic and applied research in science, technology, and engineering at colleges, universities, and laboratories in accordance with National Security Decision Directive 189.

CUI incident means improper access, use, disclosure, modification, or destruction of CUI, in any form or medium.

Information means any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, electronic, or audiovisual forms (see Office of Management and Budget (OMB) Circular No. A–130, Managing Information as a Strategic Resource).

Lawful Government purpose means any activity, mission, function, operation, or endeavor that the Government authorizes or recognizes as within the scope of its legal authorities or the legal authorities of non-executive branch entities such as state and local law enforcement.

(b) *Identifying and reporting information the contractor believes or has reason to know is potentially CUI.* This contract does not identify CUI as being involved in the contract; nonetheless:

(1) The Contractor shall notify the Contracting Officer within 8 hours of discovery if the Contractor discovers any information that the contractor believes, or has reason to know, is CUI. The potential unidentified CUI may be marked, unmarked, or improperly marked. The Contractor shall take action to appropriately safeguard any information the Contractor believes is CUI, until a Contracting Officer makes a determination.

(2) If the Contractor discovers any information that the Contractor believes is CUI and it is involved in a suspected or confirmed CUI incident, the Contractor shall notify the Contracting Officer as outlined in paragraph (b)(1), determine and inventory what CUI was or could have been improperly accessed, created, collected, used, processed, stored, maintained, disseminated, disclosed, or disposed of as part of the incident, and follow any additional incident response requirements the Contracting Officer provides if the Government determines the information is CUI.

(3) The reporting requirements of this clause do not relieve the Contractor from the requirement to follow any applicable laws, regulations, or policies outside of this clause.

(c) *Government-provided information.* The Contractor is not entitled to use Government-provided information for its own purposes, whether or not the information is marked as CUI, unless the information is in the public domain, or unless the information was lawfully made available to the Contractor by someone other than the Government.

(d) *Contractor information.* The Contractor shall appropriately identify information the Contractor owns and provides to the Government (*i.e.,* contractor bid or proposal information, contractor-attributional information, or contractor proprietary business information). The Government will determine in accordance with agency procedures whether the information provided by the Contractor is CUI or entitled to other protections (*e.g.,* contractor-attributional information associated with a CUI incident).

(1) If it is CUI or entitled to other protections, the Government will protect against the improper use or release of the information to the extent required by law.

(2) The agency may release outside the Government Contractor bid or proposal information, Contractor proprietary business information, and contractor-attributional information that is not created by or for the Government, but that is related to a CUI incident—

(i) To entities with missions that may be affected by such information;

(ii) To entities that may be called upon to assist in the diagnosis, detection, or mitigation of CUI incidents; or

(iii) For national security purposes, including cyber situational awareness.

(3) The Government may use and release Contractor bid or proposal information, Contractor proprietary business information, and contractor-attributional information, created by or for the Government and related to a CUI incident, outside of the Government for purposes and activities associated with responding to a CUI incident and for any other lawful Government purpose or activity.

(4) In any authorized release, the Government will include the Contractor proprietary business information or contractor-attributional information only to the extent necessary, as determined by the Government, to advance a lawful Government purpose or activity.

(e) *Subcontracts.* The Contractor shall include this clause, including this paragraph (e) and without alteration except to identify the parties, in all subcontracts and other contractual instruments. The Contractor shall require subcontractors to notify the prime Contractor or next higher tier subcontractor within 8 hours of discovery of a suspected or confirmed CUI incident.

(End of clause)

■ 42. Amend section 52.212–5 by—

■ a. Revising the date of the clause;

■ b. Redesignating paragraphs (b)(12) through (65) as paragraphs (b)(14) through (67) and adding new paragraphs (b)(12) and (13);

■ c. Redesignating paragraphs (e)(1)(viii) through (xxvii) as paragraphs (e)(1)(x) through (xxix) and adding new paragraphs (e)(1)(viii) and (ix);

■ d. In Alternate II:

■ i. Revising the date of the alternate; and

■ ii. Redesignating paragraphs (e)(1)(ii)(H) through (Z) as paragraphs (e)(1)(ii)(J) through (BB); and

■ iii. Adding new paragraphs (H) and (I).

The revisions read as follows:

52.212–5 Contract Terms and Conditions Required To Implement Statutes or Executive Orders—Commercial Products and Commercial Services.

* * * * *

Contract Terms and Conditions Required To Implement Statutes or Executive Orders—Commercial Products and Commercial Services (DATE)

* * * * *

(b) * * *

(12) 52.204–XX, Controlled Unclassified Information (DATE) (E.O. 13556).

(13) 52.204–YY, Identifying and Reporting Information That Is Potentially Controlled Unclassified Information (DATE).

* * * * *

(e)(1) * * *

(viii) 52.204–XX, Controlled Unclassified Information (DATE) (E.O. 13556).

(ix) 52.204–YY, Identifying and Reporting Information That Is Potentially Controlled Unclassified Information (DATE).

* * * * *

Alternate II (DATE) * * *

(e)(1) * * *

(ii) * * *

(H) 52.204–XX, Controlled Unclassified Information (DATE) (E.O. 13556).

(I) 52.204–YY, Identifying and Reporting Information That Is Potentially Controlled Unclassified Information (DATE).

■ 43. Amend section 52.213–4 by—

■ a. Revising the date of the clause;

■ b. Removing from paragraph (a)(2)(vii) ''NOV 2024'' and adding ''(DATE)'' in its place; and

■ c. Revising paragraph (b)(2)(i);

■ d. Redesignating paragraphs (b)(2)(ii) through (v) as paragraphs (b)(2)(iv) through (vii); and

e. Adding new paragraphs (b)(2)(ii) and (b)(2)(iii).

The revisions and addition read as follows:

52.213–4 Terms and Conditions—Simplified Acquisitions (Other Than Commercial Products and Commercial Services).

* * * * *

Terms and Conditions—Simplified Acquisitions (Other Than Commercial Products and Commercial Services) (DATE)

(b) * * *

(2) * * *

(i) 52.204–21, Basic Safeguarding of Covered Contractor Information Systems (DATE) (Applies to solicitations and contracts, except acquisitions solely for commercially available off-the-shelf items or Federally-funded basic and applied research in science, technology, and engineering at colleges, universities, and laboratories in accordance with National Security Decision Directive 189 when the agency does not provide any covered Federal information to the Contractor.)

(ii) 52.204–XX, Controlled Unclassified Information (DATE) (Applies to solicitations and contracts, except acquisitions solely for commercially available off-the-shelf items).

(iii) 52.204–YY, Identifying and Reporting Information That Is Potentially Controlled Unclassified Information (DATE).

* * * * *

52.227–10 [Amended]

■ 44. Amend section 52.227–10 by removing from the introductory text the phrase ''27.203–2'' and adding ''27.203–3'' in its place.

■ 45. Amend section 52.244–6 by—

■ a. Revising the date of the clause;

■ b. Removing from paragraph (c)(1)(v) ''NOV 2021'' and ''FAR clause 52.204–21'' and adding ''DATE'' and ''clause 52.204–21'' in their places, respectively; and

■ c. Redesignating paragraphs (c)(1)(x) through (xxiv) as paragraphs (c)(1)(xii) through (xxvi) and adding new paragraphs (c)(1)(x) through (xi).

The revision and additions reads as follows:

52.244–6 Subcontracts for Commercial Products and Commercial Services.

* * * * *

Subcontracts for Commercial Products and Commercial Services (DATE)

* * * * *

(c)(1) * * *

(x) 52.204–XX, Controlled Unclassified Information (DATE), if flow down is required in accordance with paragraph (e) of clause 52.204–XX.

(xi) 52.204–YY, Identifying and Reporting Information That Is Potentially Controlled Unclassified Information (DATE), if flow down is required in accordance with paragraph (e) of clause 52.204–YY.

* * * * *

PART 53—FORMS

■ 46. Revise the heading of section 53.204 to read as follows:

53.204 Administrative and information matters.

* * * * *

■ 47. Amend section 53.204–1 by—

■ a. Revising the section heading;

■ b. Removing from the introductory text the phrase ''subpart 4.4'' and adding ''4.402'' in its place;

■ c. Removing from paragraph (a) the phrase ''See 4.403 (c)(1).)'' and adding ''See 4.402–2 (c)(1).)'' in its place.

The revision reads as follows:

53.204–1 Safeguarding information and information systems (DD Form 254, DD Form 441).

* * * * *

■ 48. Add section 53.204–2 to read as follows:

53.204–2 Controlled unclassified information (CUI) Requirements (SF XXX)

SF XXX *(DATE) Controlled Unclassified Information (CUI) Requirements.* SF XXX is described in 4.403 and 11.002(i). Except for solicitations and contracts solely for the acquisition of COTS items, the contracting officer shall insert the clause at 52.204–XX, Controlled Unclassified Information, and include an SF XXX Controlled Unclassified Information (CUI) Requirements, in solicitations and contracts if the requiring activity has marked the ''Yes'' box in Part A of the SF XXX.

■ 49. Amend section 53.300 in the table following paragraph (a) by adding at the beginning of the table, the entry for ''SF XXX Controlled Unclassified Information (CUI) Requirements'' to read as follows:

53.300 Listing of Standard, Optional, and Agency forms.

* * * * *

(a) * * *

TABLE 53–1—FORMS IN THE GSA FORMS LIBRARY

Form No.	Form title
SF XXX	Controlled Unclassified Information (CUI) Requirements.
*	* * * *

* * * * *

Note: The following form, Controlled Unclassified Information (CUI) Requirements, will not be published in the CFR.

BILLING CODE 6820–EP–P

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

PAGE
1

(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

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:

(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

(c) CUI Specified.

This contract involves CUI Specified: ☐ **Yes** ☐ **No**

Following are the categories of CUI Specified and their Specified handling requirements:

- CUI Specified category name and marking:

Specify handling requirements *(for any handling aspects not described below, the requirements from paragraph (b)(i) of this section, or 32 CFR 2002.14, will apply).*

(A) Additional, non-CUI markings:

(B) Submission requirements:

(C) Physical and storage requirements:

(D) Access requirements and restrictions:

(E) Limited dissemination control markings (LDCM):

(F) Mailing and transmission requirements:

(G) Encryption requirements:

(H) Information systems and system security requirements:

(1) The CUI Specified 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.

(2) Additional system security requirements as prescribed by law, regulation or Governmentwide policy (LRGWP) for this category of CUI Specified:

(I) Destruction:

(J) Decontrol, retention, return instructions:

Add Specified Category

Remove Specified Category

SECTION II. CONTRACTOR MARKING REQUIREMENTS

The Contractor will be responsible for marking CUI identified in section I: ☐ **Yes** ☐ **No**

If yes, comply with the following marking requirements:

- CUI category name and marking:

(A) Applicable LDCMs from the CUI Registry:

(B) Any required additional CUI Specified markings from LRGWP:

Add Category

Remove Category

STANDARD FORM XXXX XX/XXXX

SECTION III. 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.

(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

PAGE
7

SECTION IV. CUI INCIDENT REPORTING REQUIREMENTS

(a) Reporting.

The Contractor is required to report all CUI incidents to:

(b) Reporting requirements.

(i) Any suspected or confirmed CUI incident must be reported within **8 hours** of discovery.

(ii) See FAR clause 52.204-XX(g) for all reporting requirements.

(c) CUI Specified incident reporting.

The following are for reporting of CUI Specified incidents:

- CUI Specified category and marking:

(A) CUI incident reporting requirements that differ from or are in addition to those in FAR clause 52.204-XX(g).

Add Category

Remove Category

PART D. APPLICABILITY OF NIST SP 800-172

The Contractor must comply with requirements from NIST SP 800-172, Enhanced Security Requirements for Protecting CUI, identified by the agency.

☐ Yes ☐ No

If yes, the agency will identify requirements for NIST SP 800-172 outside of this form. The organizational defined parameters (ODP) in Attachment 1 of this SF shall be applied for any applicable security requirements identified by the agency.

STANDARD FORM XXXX XX/XXXX

PAGE 8

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.

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 than 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.

Paragraphs (b) and (c). General Instructions

Is the CUI involved CUI Basic, CUI Specified, or both?

If the CUI involved is **CUI Basic only**, then check "Yes" at paragraph (b) and complete only the information under paragraph (b). If the CUI does not involve CUI Basic information at all, check "No" at paragraph (b).

If the CUI involved is **CUI Specific only**, then check "Yes" at paragraph (c) and complete only the information under paragraph (c). If the CUI does not involve CUI Specified information at all, check "No" at paragraph (c).

If the CUI involved is **both** CUI Basic AND CUI Specific, then check "Yes" at both paragraphs (b) and (c) and complete the information under both paragraphs.

How will the CUI Basic categories listed be handled?

All the same. If all of the categories of CUI Basic will be handled identically, fill out the information for subparagraph (i) (see (b)(i) below). Subparagraph (ii) will not apply; enter "n/a" in the "CUI Basic category name and marking" fill-in field at subparagraph (ii).

At least one different. If some of the categories of CUI Basic will be handled identically, and one or more will have unique handling requirements, fill out the information for subparagraph (i) for the categories that will be handled the same (see (b)(i) below). For the one or more categories that have unique handling requirements, fill out the information in subparagraph (ii) (see (b)(ii) below).

All different. If all CUI Basic categories have unique handling requirements, fill out the information for subparagraph (ii) (see (b)(ii) below). Subparagraph (i) will not apply; enter "n/a" in the "access and dissemination requirements" fill-in field.

(b)(i) CUI Basic that will be handled identically

(1) **Enter access and dissemination requirements in the fill-in field.** Enter any limited dissemination control marking (LDCM) or lawful Government purpose (LGP) restriction that applies to the CUI and any prerequisites they create before someone can access the CUI. Also itemize how the contractor must comply with the restrictions, and, for any LDCM that includes lists or other similar information, include that additional information for each. Also include any access requirements, restrictions, or approval processes for access that the contractor must follow because of the LDCM.

(2) **Enter information systems and system security requirements.** Check one or more of the boxes that apply to the information. CUI Basic will be on either a Federal information system, a non-Federal information system, or both types of information systems.

If any of the CUI Basic is on a Federal information system(s) operated "on behalf of an agency", list all of the Federal information systems in the fill-in field. Use system names to identify multiple Federal information systems to distinguish clearly between them. In the accompanying requirements document, set out applicable requirements from NIST SP 800-53 ensuring that the system is configured to no less than moderate confidentiality impact level.

Checking "Non-Federal information system(s) (contractor's internal IT system)," means the contractor will apply NIST SP 800-171 Revision 2 requirements. If cloud computing services will be used, see FAR clause 52.204-XX(d)(5)(i)(B).

If the agency wants the contractor to apply additional controls beyond the NIST SP 800-171 Revision 2 to address requirements higher than the moderate confidentiality level, check the subparagraph and insert the location of the additional requirements. The additional controls must be in the accompanying requirements document in accordance with 32 CFR 2002.14(h)(2).

(3) **Enter decontrol, retention and return instructions in the fill-in field.** Identify any: instructions for handling CUI Basic with a "destroy by" date; automatic decontrol situations that apply and what the contractor should do in the automatic decontrol situation; and instructions regarding whether the contractor will retain the CUI or return it to the agency (either during the contract or upon termination), by when, via what method, etc. Instructions may also include records management instructions and instructions for transferring CUI to the National Archives.

(b)(ii) CUI Basic categories with unique handling requirements

In this subparagraph, enter the handling information for the CUI Basic categories with unique handling requirements. Only identify in the subparagraphs the handling requirements that differ from the CUI Basic requirement.

Enter one CUI Basic category that has unique handling requirements in the "CUI Basic category name and marking" fill-in field. Use the instructions for the equivalent subparagraphs under (b)(i) above.

Use the "Add Basic Category" button to create an entry for each category with differing handling requirements.

(c) CUI Specified categories

If CUI Specified is involved, check "Yes" to "This contract includes CUI Specified."

Enter the CUI Specified category name and marking in the "CUI Specified category name and marking" fill-in field. The information for the CUI Specified category will need to be entered in subparagraphs (A) to (J). Include only requirements established by the authorizing law, regulation or Governmentwide policy (LRGWP). The requirements from section I(b)(i), 32 CFR 2002.14 will apply for any handling aspects not described in subparagraphs (A) to (J).

For elements that do not have a CUI Specified requirement, enter "See CUI Basic" to use the CUI requirements for that element. For elements (A) and (B), there is no CUI Basic equivalent; enter "n/a" or "none" if there is no CUI Specified requirement.

For elements (D), (H), and (J), the agency may instead enter "See requirements in section I(b)(ii) [(A), (B), or (C)]" (respectively), if the agency already entered requirements there and wants to use the same ones here. Be sure to also state which category if there is more than one listed under section I(b)(ii).

Enter the CUI Specified requirements as follows:

(A) Additional, non-CUI markings: Some authorities for CUI Specified include requirements for warning banners, indicators, and other similar additional markings. If the contractor is required to take action in response to these markings, or required to add these markings to the information, identify the markings in the fill-in field with any accompanying actions triggered by the markings or accompanying lists that the contractor must be aware of. List actionable additional markings only.

(B) Submission requirements: Some authorities for CUI Specified include requirements for how the CUI must be submitted to the agency such as in an envelope, or via a formal request to withhold the information from the public. Include such LRGWP requirements applicable to this category.

(C) Physical and storage requirements: Identify any physical security or storage requirements the LRGWP requires for this category.

(D) Access requirements and restrictions: Identify the following when it is in furtherance of a lawful Government purpose for the contractor to permit access to the CUI (including to support contract performance):

- Restrictions on access to the CUI,
- Limited dissemination requirements in the LRGWP (these are not the same as CUI limited dissemination controls on the CUI Registry that the agency chooses to apply; those are identified under paragraph (E) below),
- Approval process for access,
- Lists of authorized individuals, and
- Procedures the LRGWP requires the contractor to follow before permitting or restricting access to the CUI.

(E) Limited dissemination control markings: Identify any limited dissemination control markings (LDCMs) from the CUI Registry that apply to the CUI Specified information and itemize how the contractor must comply. For any LDCM that includes lists or other similar information, include the additional information for each. Enter "none" if the agency chooses not to apply an LDCM to this category.

(F) Mailing and transmission requirements: Include any applicable LRGWP requirements for physical mailing/transmission and electronic mailing/transmission, as appropriate.

(G) Encryption requirements: Some CUI Specified LRGWPs contain requirements for encrypting the CUI. Identify those requirements, their standards, and the circumstances in which they apply (such as while the electronic information is at rest, while in transit, or both).

(H) Information systems and system security requirements: Identify the type of information system, either Federal information system (operated "on behalf of the agency") or non-Federal information system, and associated system security requirements at FAR clause 52.204-XX, Controlled Unclassified Information. Use the instructions for the equivalent subparagraph under (b)(i)(2) above but substitute CUI Specified requirements for the CUI Basic requirements.

(I) Destruction: Include any requirements for destruction contained in the applicable LRGWP.

(J) Decontrol, retention, return instructions: Identify category-specific instructions for handling the CUI Specified category. If it has a "destroy by" date, identify category-specific automatic decontrol situations that apply and what the contractor should do in the automatic decontrol situations. Any instructions regarding whether the contractor will retain the CUI or return it to the agency (either during the contract or upon termination), by when, via what method, etc. Include any LRGWP requirements for decontrol, retention, or return. Instructions may also include records management instructions and instructions for transferring CUI to the National Archives.

Use the "Add Specified Category" button to create an entry for each CUI Specified category.

SECTION II. CONTRACTOR MARKING REQUIREMENTS.

Will the contractor be responsible for marking the CUI identified in section I?

If no, the contractor will not be responsible for marking the CUI. Check "No" and proceed to section III.

If yes, the contractor will be responsible for marking the CUI, then check "Yes" to "Contractor will be responsible for marking CUI identified in section I," and proceed with completing section II.

Enter the marking requirements. Enter a category name and category marking in the "CUI category name and category marking" fill-in field. Markings must be applied in accordance with 32 CFR part 2002, the CUI Registry at https://www.archives.gov/CUI, and the CUI Marking Handbook. If the contractor will be marking all categories, and marking them all the same way, enter "All CUI identified in section I." The information for the CUI category will need to be entered in subparagraphs (A) and (B).

(A) Applicable Limited Dissemination Control Markings (LDCMs) from the CUI Registry: List in the fill-in field any applicable LDCM the contractor will be required to apply to the category.

(B) Any required additional CUI Specified markings from law, regulation, or Governmentwide Policy (LRGWP): List in the fill-in field any additional markings required by LRGWP that the contractor will be required to apply to the category. These may include warning statements and indicators if the LRGWP requires them.

Use the "Add Category" button to create an entry for each CUI category with marking requirements.

SECTION III. TRAINING REQUIREMENTS.

(a) Provide general training information.

(i) All contractor employees must take general CUI training prior to accessing CUI. They must also complete refresher training not less often than 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 initial general CUI training if they have received 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). 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 clause 52.204-XX(f)(2)(i), check "Yes" and complete the information. If there are no additional training requirements, check "No." Note, privacy training is required by FAR clause 52.224-3 for contractor employees and should not be identified as additional training in the SF.

Enter a 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, contractor may use training developed by third parties).

(D) Select from the drop-down box the frequency with which the 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 by checking the appropriate box(es) (i.e., submit employee training details, employee testing, or refresher training). If the exemption waiver is not allowed, check the last box.

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

SECTION IV. CUI INCIDENT REPORTING REQUIREMENTS.

(a) Reporting.

Enter the single agency point of contact or website to which the contractor must report any CUI incidents in the fill-in field (i.e., name, email address, and phone number, or website Universal Resource Locator (URL)).

When the CUI involved is located at a non-Federally-controlled facility, the contractor will report all incidents as identified in the fill-in field.

(b) Reporting requirements.

No additional information is needed for this paragraph.

(c) CUI Specified incident reporting.

For each CUI Specified category identified in section I(c), provide the incident reporting requirements that differ from, or are in addition to, those in FAR clause 52.204-XX. If CUI Specified is not expected to be handled under the contract, enter "n/a" or "none" in the "CUI Specified category and marking" fill-in field.

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

PART D. APPLICABILITY OF NIST SP 800-172

Does the contractor have to comply with any requirements in NIST SP 800-172?

If no, the CUI will NOT require compliance with any requirements of NIST SP 800-172, then check "No". Stop here.

If yes, then check "Yes" and the agency must identify in the solicitation and contract the NIST SP 800-172 requirements the offeror or contractor must comply with. The organizational defined parameters (ODPs) in Attachment 1 of this SF shall be applied for any applicable security requirements identified by the agency.

Note: Information system owners (i.e., contractor or subcontractor) will set specific security requirements for some of the security requirements. See Attachment 1 of this SF.

Attachment 1: Organizational Defined Parameters (ODP) for NIST SP 800-172

The ODPs provided in the bold text below shall be applied for any security requirements identified by the agency.

Specific security requirements to be defined by the information system owner (i.e., contractor or subcontractor) are identified in bracketed bold text.

800-172ID	Security Requirement with ODP Value
3.1.3e	Employ **secure information transfer solutions** to control information flows between security domains on connected systems.
3.2.1e	Provide awareness training **upon initial hire, following a significant cyber event, and at least annually** focused on recognizing and responding to threats from social engineering, advanced persistent threat actors, breaches, and suspicious behaviors; update the training **at least annually** or when there are significant changes to the threat.
3.2.2e	Include practical exercises in awareness training for **all users, tailored by roles, to include general users, users with specialized roles, and privileged users** that are aligned with current threat scenarios and provide feedback to individuals involved in the training and their supervisors.
3.4.2e	Employ automated mechanisms to detect misconfigured or unauthorized system components; after detection, **remove the components or place the components in a quarantine or remediation network** to facilitate patching, re-configuration, or other mitigations.
3.5.1e	Identify and authenticate **systems and system components, where possible** before establishing a network connection using bidirectional authentication that is cryptographically based and replay resistant.
3.6.1e	Establish and maintain a security operations center capability that operates **24/7, with allowance for remote/on-call staff**.
3.6.2e	Establish and maintain a cyber incident response team that can be deployed by the organization within **24 hours**.
3.9.1e	Conduct **[organization-defined enhanced personnel screening to be defined by information system owner (i.e., contractor or subcontractor)]** for individuals and reassess individual positions and access to CUI **[organization-defined frequency to be defined by information system owner (i.e., contractor or subcontractor)]**.
3.11.1e	Employ **threat intelligence, at a minimum from open or commercial sources, and any Federally provided sources** as part of a risk assessment to guide and inform the development or organizational systems, security architectures, selection of security solutions, monitoring, threat hunting, and response and recovery activities.
3.11.2e	Conduct cyber threat hunting activities on an **on-going aperiodic basis or when indications warrant** to search for indicators of compromise in **organizational systems** and detect, track, and disrupt threats that evade existing controls.
3.11.5e	Assess the effectiveness of security solutions **at least annually or upon receipt of relevant cyber threat information, or in response to a relevant cyber incident** to address anticipated risk to organizational systems and the organization based on current and accumulated threat intelligence.
3.11.7e	Develop a plan for managing supply chain risks associated with organizational systems and system components; update the plan **at least annually, and upon receipt of relevant cyber threat information, or in response to a relevant cyber incident**.
3.12.1e	Conduct penetration testing **at least annually or when significant security changes are made to the system**, leveraging automated scanning tools and ad hoc tests using subject matter experts.
3.13.1e	Create diversity in **[organization-defined system components to be defined by information system owner (i.e., contractor or subcontractor)]** to reduce the extent of malicious code propagation.
3.13.2e	Implement the following changes to organizational systems and system components to introduce a degree of unpredictability into operations: **[organization-defined changes and frequency of changes by system and system component to be defined by information system owner (i.e., contractor or subcontractor)]**.

800-172ID	Security Requirement with ODP Value (continued)
3.13.3e	Employ **[organization-defined technical and procedural means to be defined by information system owner (i.e., contractor or subcontractor)]** to confuse and mislead adversaries.
3.13.4e	Employ **physical isolation techniques or logical isolation techniques or both** in organizational systems and system components.
3.13.5e	Distribute and relocate the following system functions or **resources [organization-defined frequency to be defined by information systems owner (i.e., contractor or subcontractor)]: [organization-defined system functions or resources to be defined by information system owner (i.e., contractor or subcontractor)]**.
3.14.1e	Verify the integrity of **security critical and essential software** using root of trust mechanisms or cryptographic signatures.
3.14.3e	Ensure that **specialized assets including Internet of Things (IOT), Industrial Internet of Things (IIOT), Operational Technology (OT), Government Furnished Equipment (GFE), Restricted Information Systems, and test equipment** are included in the scope of the specified enhanced security requirements or are separated in purpose-specific networks.
3.14.4e	Refresh **[organization-defined systems and system components to be defined by information system owner (i.e., contractor or subcontractor)]** from a known, trusted state **[organization-defined frequency to be defined by information system owner (i.e., contractor or subcontractor)]**.
3.14.5e	Conduct reviews of persistent organizational storage locations **not less than annually** and remove CUI that is no longer needed.
3.14.6e	Use threat indicator information and effective mitigations obtained from **at a minimum, open or commercial sources, and any Federally provided sources** to guide and inform intrusion detection and threat hunting.
3.14.7e	Verify the correctness of **[organization-defined security critical or essential software, firmware, and hardware components to be defined by information system owner (i.e., contractor or subcontractor)]** using **[organization-defined verification methods or techniques to be defined by information system owner (i.e., contractor or subcontractor)]**.

[FR Doc. 2024–30437 Filed 1–14–25; 8:45 am]
BILLING CODE 6820–EP–C