2101 Wilson Boulevard, Suite 700, Arlington, VA 22201-3060 • (703) 522-1820 • (703) 522-1885 Fax • NDIA.org

March 17, 2025

Mr. Michael O. Jackson
Procurement Analyst
General Services Administration

Electronic Submission: www.regulations.gov, FAR Case 2017-016

Re: NDIA Comments on Proposed Rule to amend the Federal Acquisition Regulation to implement the National Archives and Records Administration's Controlled Unclassified Information Program.

Dear Mr. Jackson:

The National Defense Industrial Association (NDIA) appreciates the opportunity to provide comments on the proposed rule to amend the Federal Acquisition Regulation (FAR) to implement the National Archives and Records Administration's (NARA's) Controlled Unclassified Information (CUI) Program.

NDIA is the nation's largest defense industry association, representing over 1,700 corporate and over 67,000 individual members from small, medium, and large contractors, a majority of which are small businesses. Our members engage daily with the federal government's national and homeland security apparatuses. They are well-versed in the array of cybersecurity requirements and implementation challenges.

NDIA and its member companies are committed to securing the data and systems that power the defense industrial base (DIB), as well as the platforms, infrastructure, and services that support our nation's warfighters. Simultaneously, to avoid extraneous costs and burdens on industry, NDIA has been attentive to focusing resources and efforts to prioritize protecting the critical information and systems that truly matter. To that end, NDIA supports the idea of a harmonized federal rule to govern the handling of CUI for all agencies and contractors.

As a general comment, NDIA would note and caution that this rule does not simplify, clarify, or harmonize the existing cybersecurity requirements prescribed on the DIB, so while beneficial, it is adding to the compliance burden and raising the cost of entry and sustainment for contractors. NDIA strongly believes that as part of any effort to strengthen the protections and mitigations we place on government data and systems, we should be focused on standardizing and harmonizing such requirements to the greatest degree practicable and work to lessen the burden on companies that wish to support the government mission. Without such a focus, we are only adding to the complexity of a patchwork of protection and compliance.

Improvements Needed for the Proposed SF XXX Form

NDIA supports the concept of the proposed standard form (SF) XXX and believes it could be beneficial with updates to help both the government and contractors identify and manage CUI more consistently. Such a form, however, must serve to streamline and facilitate the process and ensure that agencies do

not use the form to create additional opportunities to impose agency-specific requirements or demonstrations. The form should be limited to include only elements of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 or 800-172 and demonstrations through reporting to DIBNET. To ensure that the government and contractors can derive such benefits from a final form, the government should afford industry engagement and provide a public comment period during its development.

Additionally, the current Department of Defense Form 254 (DD254) also has a section outlining contractor requirements to protect CUI information. The new form should provide clarity to contractors who may be handling CUI in a classified program and offer direction when there may be conflicting guidance between the new SF XXX and the DD254.

Cost Estimates Undervalue Industry Costs for Compliance

NDIA continues to believe that the government misunderstands and underestimates the costs associated with the adoption, integration, and maintenance costs of the NIST SP 800-171 & 800-172. That misunderstanding and the corresponding underestimation of costs are repeated in this proposal. NDIA would provide for the record of the promulgation of this proposal the details of a cost survey it conducted in 2024 and published as part of the NDIA *Vital Signs 2025* report (pg. 32 et seq). We would note that the estimations for costs in this rule do not align with the experience NDIA is measuring in their membership and identifying across the entire DIB. As further evidence of the continuation of that misunderstanding and cost underestimation, we would like to share the following new information developed in response to this FAR proposal.

An NDIA member company conducted a survey of the proposed rule that included 61 respondents from both defense and non-defense contractors, which offers some unique insights. A high number of respondents have had issues with customer confusion about CUI (close to 70%), over-classification of CUI (close to 65%), and receiving unmarked CUI (close to 55%). For the commonly identified risks, only 31% of respondents believe contracting officers will have time to deal with the mandated reporting, over 60% believe contract and delivery delays are likely, and the majority believe CUI will be mismarked and customer staff will not be properly trained.

The survey also addressed the estimated contractor training costs, which do not include costs related to technology controls and reporting systems. On average, the respondents estimated the average annual training cost per employee will be $5,425. Additional member company estimates place the range at $400 to $600 annually for those employees involved in handling CUI. This is in stark contrast to the $76 per employee estimate for training costs included in the proposed rule.

The CUI Incident Notification Timelines are Too Short and Must be Extended

Under the proposed FAR provisions, a contractor must inform the agency (or higher tier contractor if a subcontractor) within 8 hours of the discovery of a suspected or confirmed CUI incident, suspected CUI not listed on the SF XXX form, improperly marked CUI, or an inconsistency between SF XXX and the appropriate CUI clause. This timeframe is too narrow and does not align with other reporting

requirements that the government has been embracing and adopting across a host of cyber, software, and supply chain requirements. Cybersecurity incidents involve a multi-phase process that includes recognition, research, response, resolution, and reporting. Given the complexity of these incidents, resolution often takes weeks or months.

NDIA recommends that the 8-hour reporting timeframe be extended to 72 hours to comport with the rapid reporting timeline of a cyber incident under DFARS 252.204-7012 to provide ample time for fact-finding and reporting, as well as consistency with other similar reporting requirements. Liability protections are also required to incentivize companies, focusing on situational awareness, resilience, and protection over incident victimization for criminal and judicial litigation.

Finally, the government must clearly define the essential reporting information required within the timeframe. Without such specificity, organizations may struggle to balance timely reporting with accuracy, potentially leading to incomplete or misleading initial reports. A well-defined reporting standard should focus on critical, actionable details—such as the nature of the incident, affected systems, and immediate mitigation steps—while allowing subsequent updates as the investigation progresses. This approach ensures compliance with reporting mandates without compromising the effectiveness of the incident response process.

We would also note the opportunity for confusion in the government and with contractors regarding the inclusion of mismarked or unmarked CUI. If the government fails to mark or it mismarks the data it wishes to protect, then industry will struggle to determine what should or should not be protected and could overwhelm any reporting process in an effort to ensure that all possible CUI data is identified for adequate protection. NDIA would recommend the limitation of reporting to only information that is clearly marked CUI, in order to avoid overwhelming the process.

CUI Incident Definition Should Clearly Identify Exclusions for Clarity

In the proposed FAR changes, the definition of a CUI Incident is quite broad, but within the specific regulations, they repeatedly state that "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." For clarity, such a refining statement should be included with the definition or at least placed alongside the definition so the scope of what constitutes a CUI incident is clear.

The rule should establish a permissive environment that is conducive to proactive reporting that enables the safeguarding of sensitive information. The term "incident" has meaning and, if reported before confirmation that the requirements are met, could result in negative consequences for the reporting party despite their good intentions. Therefore, we recommend the word "incident" be dropped until after confirmation of a qualifying incident.

Lack of Appropriate Scoping

The proposed rule lacks many appropriate boundaries. One example is operational technology (OT) items. The vast majority of specialized equipment (CNCs, Lab Equipment, industrial equipment, and

more) runs on legacy Operating Systems and Software due to the need for a standard baseline across hundreds or thousands of the same equipment along with the need for equipment to run stably around the clock, all year long, for years on end. The NIST Cyber Security Framework (CSF) and Risk Management Framework (RMF), with mapping for nonfederal systems, establish flexible and risk-based selections for systems development and throughout the operational life cycle, including evaluation across strategy, planning, maintenance, and sunsetting. NDIA recommends considering actions aligned to risk management that include critical aspects such as resource allocation and availability, threats, attack scenarios with mitigations, resiliency, metrics, and conditions for deployed international platforms. Additionally, consideration of other international frameworks would further ensure compliance and preparation of the global industrial base.

The Proposal is Not Aligned with the CUI Protection Provisions of the NISPOM

In DoD Directive 5015.42, the Defense Counterintelligence and Security Agency (DCSA) was given the charter to oversee CUI when CUI is co-mingled with classified materials controlled by the National Industrial Security Program Operating Manual (NISPOM). The Directive states that DCSA "Administers the CUI Program in the [National Industrial Security Program] NISP in accordance with DoDI 5200.48 and for CUI protected by provisions of contracts requiring access to classified information" and "Provides security assistance and guidance to the DoD Components on the protection of CUI when DoD Components establish CUI requirements in DoD classified contracts for NISP contractors falling under DCSA security oversight."

This would seem to create a conflict by indicating that DCSA could have cognizance over and audit CUI affiliated with classified programs. Such cognizance is in addition to the agency that owns the CUI, which could lead to double audits for contractors who hold that information and force an undue burden on industry. It also creates the opportunity for misalignment and differing conclusions on the efficacy of the protections a contractor may impose to protect CUI when in a classified program. NDIA would recommend that DIBCAC be the cognizant entity for CUI data in all instances where it may appear.

Lack of Acknowledgment of External Service Providers (ESP)

The proposed rule acknowledges the subject of Cloud Service Providers (CSPs), but it does not acknowledge that the vast majority of businesses rely on third-party IT services companies. Enterprise Service Providers (ESPs) provide a critical element in the implementation of NIST SP-800-171 for their customers and routinely are a target of malicious actors. As an example, in the DoD implementation of CMMC, ESPs are required to implement NIST SP 800-171 on their networks and systems in order to provide certain services to their CUI clients. Also, ESPs do not interact with any specific contract and would not be subject to flow-down requirements. NDIA recommends that the External Service Provider definition and Requirements be adopted wholly as they are defined by FedRAMP and shared responsibility matrices per data categorization and role/responsibility for safeguarding.

2101 Wilson Boulevard, Suite 700, Arlington, VA 22201-3060 • (703) 522-1820 • (703) 522-1885 Fax • NDIA.org

Clarify FedRAMP Moderate Baseline as Authorized

In Part 52, Controlled Unclassified Information, the term FedRAMP Moderate Baseline is used. Various Third-Party Party Assessment Organizations (ISO, SOC, CMMC) and even government entities at times incorrectly interpret this to mean FedRAMP Moderate Authorized CSPs. This situation came to light in the operational mechanisms for DFARS 252.204-7012. Equivalency was made virtually impossible and caused some companies to suddenly fail DoD assessments due to vagueness and misinterpretations. To prevent this potential problem, NDIA requests the term be clarified to say FedRAMP Moderate Authorized or equivalent via company due diligence of the shared responsibility matrices. CSPs are not limited by country-specific boundaries, and additional baselines should include equivalency for global cloud standards as applicable.

Update the CUI Definition to Resolve Ambiguities in the Scope of CUI Regulations

While the proposed definition of CUI in FAR 2.101 contains carveouts to limit the impact of CUI regulations, they are insufficient to prevent the unintended consequence of CUI regulations imposing additional requirements on how contractors, including small businesses, handle their own proprietary information. While the CUI definition has a robust carveout for college and university research, the definition's carveout for information a contractor possesses that is from non-government sources or unrelated to government contracts is not robust enough to preclude CUI requirements from being extended to such data. Specifically, a contractor's information merely possessed by the government outside the scope of any government contract is not included in a carveout and may be treated as CUI. The broad imposition of CUI's information security requirements (e.g., NIST SP 800-171) upon how industry treats its own proprietary or trade secret information, beyond such information created for the government, results in the imposition of information security requirements over and above the standard industry processes. The proposed changes to the FAR 2.101 CUI definition, which should be carried through FAR 52.204-XX(a), FAR 52.204-YY(a), and other provisions defining CUI, should be the following:

> 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 specifically 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; or
> (5) Technical data or computer software pertaining to commercial products or commercial services.

Furthermore, the updates to FAR 9.505, 9.505-4, and 9.508 make clear proprietary information is contractor-proprietary business information and may help contractors determine if their data will or will not become governmental property.

Offeror Marking of CUI

We must be careful about the FAR inadvertently imposing protection requirements, along with marking requirements, upon contractors to label and protect their own information as CUI to meet a government protection requirement, even before it is provided to the government. This is especially true in instances in which the information is treated as CUI simply because it is a company's proprietary information or bid and proposal information. It is troublesome that the government is forcing the offerors or contractors to label information being provided to the government as CUI without clear boundaries as to the scope of when such information should be labeled. This is contrasted with a clear boundary of the government attaching a CUI cover page to a contractor's proprietary information to designate it as CUI within the government.

With the FAR requiring protection of such information labeled CUI, without clear and reasonable boundaries for the treatment and protection of a company's own proprietary information, such protections would ultimately drive unnecessary cost and complexity into doing business with the government and result in further erosion of the government contracting industrial base. An ideal solution to this would be to maintain the requirement of marking CUI information as an inherently governmental function in line with FAR 7.503(c)(5). At a minimum and to help alleviate concerns, NDIA proposes that the CUI definition be modified to provide a clear boundary to the marking requirements in the SF XXX, with instruction and training for government program and contract representatives.

Application of CUI requirements to Commercial Products in Contracts of Any Value but Not to COTS Items.

Although the FAR proposed language has a distinct carveout for information associated with Commercial Off-the-Shelf Items (COTS), the language seems to have a contradiction by stating that CUI requires protection, regardless of dollar value or commerciality of the product or service. This creates confusion about the meaning of the definition and seems to state that the rule would apply to contracts at or below the Simplified Acquisition Threshold (SAT), as well as to commercial products and commercial services, which would include COTS.

Instead of making an artificial distinction between commercial products and commercial services and COTS items (a subset of commercial items), government-specific CUI safeguarding requirements should not be leveraged on suppliers for commercial products or commercial services in general. COTS items can also come with proprietary supplier information. If it is in the government's interest to protect proprietary data from suppliers from required government disclosure, then the government must protect such data when it is received but should not levy those safeguarding requirements upon the commercial marketplace prior to receipt of such data. Such an action effectively requires the commercial marketplace to change to meet the government instead of the government taking advantage of efficiencies in the commercial marketplace.

Furthermore, the imposition of such requirements upon the commercial marketplace will result in the loss of contractors willing to do business with the government and ultimately create a loss of available technologies offered to the government, an increase in the costs of government procurement with little benefit, or both. The FAR Case already acknowledges that an offeror/contractor "usually marks its proprietary information as a best business practice to protect its own interests and information," so the government should impose CUI requirements on its own handling of such data but not extend such requirements to an offeror/contractor of commercial products and commercial services. This enables the offeror/contractor to implement their own best practices for protecting their own proprietary information.

Application of CUI Requirements to Patent Applications

The FAR proposal includes language requiring the protection of patent applications such as CUI. While it is understandable that the U.S. Patent and Trademark Office and the U.S. Government want to safeguard patent applications when handling an unpublished or draft patent application, it must be careful about the updated FAR 27.203-1 inadvertently imposing contractor/inventor restrictions under the guise of imposing protection of patent applications and patent-related materials as CUI. If this becomes the case, there are widespread ramifications that are especially highlighted in areas where research is being conducted without substantial inherent capital resources or information security infrastructure. For example, small businesses filing patent applications may not have sufficient facility protections, information security protections, or the resources to invest in or create such capabilities, and this proposal may force them to upgrade their equipment and systems simply because they seek to protect their own innovations developed under SBIR/STTR programs by filing a patent application. These additional requirements may encourage small businesses to not file a patent application on their innovations, thereby not securing the government's investment in such entities or even disincentivize small business participation in SBIR/STTR programs.

Potential for Multiple Agencies to Interpret NIST Differently

This rule allows agencies to perform assessments of contractors. However, it lacks a central body to harmonize and align those assessments and the conclusions they may make. This could lead to there being differing or misaligned interpretations of NIST requirements between agencies. In order to facilitate harmonization and alignment of interpretations and conclusions related to assessments, NDIA would propose that reciprocity or equivalency needs to be established as appropriate for existing domestic and global government-recognized cyber security assessment methodologies to enable federal and international economies of scale regarding cybersecurity and resilience.

International Standards Organization's ISO 27000 Series for Information Security includes information security management, audit and certifications, monitoring, governance, telecommunications, and cloud services. International reciprocity could support U.S. international subcontractors for cross-sector industries and markets. NIST is a participant in international cyber entities, including standards mapping and global assessment organizations, with mapping to the ISO standards.

2101 Wilson Boulevard, Suite 700, Arlington, VA 22201-3060 • (703) 522-1820 • (703) 522-1885 Fax • NDIA.org

Cybersecurity and Impacts to the U.S. Supply Chain & Small Business

The U.S. is at continued risk of a diminishing supplier base as small companies are not considering government solicitations and contracts due to complexity and as profitability is more readily realized in adjacent or more concerning global (friendly and adversary) markets. The regulation, as proposed, does not extend cybersecurity resiliency as there are no incentives for suppliers and small businesses. Additional assistance could be offered through tax credits and the creation of an incentive to create cybersecurity resilience and mitigations over validation assessments across markets, including manufacturing or the creation and finding of a small business and government partnership, single entity consortium to provide solutions, lower costs, and provide professional services as to architecture, controls, and monitoring for the supply chain and manufacturing.

Conclusion

NDIA and its membership support the government's desire to promote a strong, dynamic, and robust defense industrial base. We thank you for the opportunity to submit these comments and for your attention to the recommendations provided to improve the proposed FAR CUI regulation. If you have any questions related to these comments, please reach out to Michael Seeds at mseeds@ndia.org.

Sincerely,

National Defense Industrial Association