



March 17, 2025

General Services Administration  
Regulatory Secretariat Division  
ATTN: Mr. Michael O. Jackson, 202-821-9776, [michaelo.jackson@gsa.gov](mailto:michaelo.jackson@gsa.gov)

RE: FAR Case 2017-016: *Controlled Unclassified Information*

Dear Mr. Jackson:

On behalf of the Aerospace Industries Association (AIA)<sup>1</sup>, in response to the request for public comments to the FAR proposed rule regarding *Controlled Unclassified Information*, I am pleased to offer the enclosed comments matrix along with the following priority comments and recommendations which are also included in the enclosed comments matrix:

#### Priority Comments & Recommendations

##### **1) Revise the CUI Definition to Resolve Ambiguities in the Scope of CUI Regulations.**

Although 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 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 carveout for information a contractor possesses from non-Government sources or unrelated to Government contracts is not robust enough to preclude CUI requirements from being extended to such information. Specifically, contractor information merely possessed by the Government outside the scope of any Government contract is not included in a carveout and therefore 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 standard industry processes used to protect its own information.

Of note, correctly identifying, defining, marking and delivering information as CUI is an inherently governmental function. It is imperative that we are careful about the FAR levying protection/marketing requirements to force contractors to broadly label and protect their own information as CUI to meet a government protection requirement before providing it to the Government. Such requirements would ultimately drive unnecessary cost and complexity into doing business with the Government resulting in further erosion of the Government contracting industrial complex.

Proposed changes to 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, are as follows:

**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**

---

<sup>1</sup> Founded in 1919, the Aerospace Industries Association (AIA) is the premier trade association advocating on behalf of over 280 aerospace and defense (A&D) companies for policies and investments that keep our country strong, bolster our capacity to innovate and spur economic growth. AIA's members represent the nation's leading aerospace and defense manufacturers and suppliers of civil, military, and business aircraft and engines, helicopters, unmanned aerial systems, space systems, missiles, equipment, services, information technology, and other related components.

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.

## 2) Application of CUI requirements to Commercial Products and Commercial Services.

Although the proposed rule exempts information associated with Commercial Off the Shelf (COTS) items, the language contradictorily states that “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 [simplified acquisition threshold] SAT and to commercial products and commercial services.”

If the Government’s interest is to protect proprietary supplier information from required Government disclosure, the Government must protect such information when it is received but should not levy those safeguarding requirements upon the commercial marketplace. Such an action effectively requires the commercial marketplace to change to meet the Government rather than the Government taking advantage of efficiencies in the commercial marketplace. Furthermore, the imposition of such requirements upon the commercial marketplace will result in loss of contractors willing to do business with the Government, loss of available technologies, and ultimately an increase of costs of Government procurement with little added benefit.

The proposed rule acknowledges that an offeror/contractor “usually marks its proprietary information as a best business practice to protect its own interests and information.” Recognizing this standard practice, AIA recommends the Government impose CUI requirements on its own handling of such information but not extend such requirements to an offeror/contractor of commercial products and services. Additionally, rather than creating an artificial distinction between commercial items and COTS items (a subset of commercial items – which can also come with proprietary supplier information), AIA recommends that Government-specific CUI safeguarding requirements should not be imposed on suppliers for commercial products or commercial services broadly.

## 3) “CUI Incident” Definition Should More Clearly Identify Exclusions.

In the proposed rule, the definition of a “CUI incident” is very broad, stated as: “suspected or confirmed improper access, use, disclosure, modification, or destruction of CUI.” However, the rule also repeatedly clarifies elsewhere 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 within the definition so the scope of what constitutes a CUI incident is clear.

Additionally, AIA recommends the removal of the term “incident” for reports associated with CUI before they are confirmed to be “incidents.” Companies that seek to be responsible stewards of CUI information may make reports that turn out not to qualify as “incidents” and

## **RE: FAR Case 2017-016: *Controlled Unclassified Information***

could face consequences for their actions despite having been found to not have reported a qualifying incident.

### **4) CUI Incident Notification Timelines are Impractical 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 the SF XXX and the appropriate CUI clause. The 8-hour reporting requirement is a very limited timeframe and would prove challenging in implementation, likely resulting in non-compliance. To avoid such situations, AIA recommends that the 8-hour reporting timeframe be extended to 72 hours to provide ample time for fact-finding and reporting as well as consistency with other similar reporting requirements. The 72-hour timeline is consistent with other urgent reporting requirements, such as the requirement to report cyber incidents under DFARS 252.204-7012.

Regarding 52.204-WW, Notice of Controlled Unclassified Information Requirements, paragraph (d), Unmarked CUI or mismarked CUI, requires that an "Offeror should notify the Contracting Officer within 8 hours of discovery of any CUI that is not marked, not properly marked, not identified on the SF XXX form, or is involved in a suspected or confirmed CUI incident." As per the proposed rule, unmarked or mismarked CUI is not a "CUI incident" and therefore should not be subject to same reporting timeline as true "CUI incidents." Since 32 CFR Part 2002 and NARA guidance requires the Government to mark information as CUI, contractors should not be made responsible for an inherently governmental function and do not have the authority to independently validate and mark Government's determinations. AIA recommends that to the extent contractors are required to notify the Government of potential marking issues, 10 working days should be sufficient to do so.

### **5) Application of CUI Requirements to Patent Applications.**

The FAR proposed rule includes language requiring protection of patent applications as CUI. While it is understandable that the Government wants to safeguard patent applications when handling an unpublished or draft patent application, it must be careful about the updated FAR 27.203-1 imposing additional requirements on contractor/inventor protection of patent applications and patent-related materials once they are designated as CUI. If this becomes the case, there are widespread ramifications that are especially highlighted in areas where research is being conducted without significant capital resources or information security infrastructure. For example, small businesses filing patent applications may not have sufficient facility protections, information security protections, or resources, and may be forced to upgrade their equipment and systems simply because they seek to protect their own innovations developed under SBIR/STTR programs. These additional requirements may ultimately encourage small businesses to not file on their innovations, not securing the Government's investment in such entities, or even chill small business participation in SBIR/STTR programs.

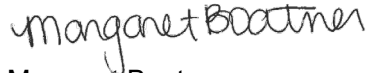
### Conclusion

Lessons learned demonstrate how requirements and processes in cybersecurity are mutually beneficial when shared through robust collaboration across sector business operations representing all stakeholders. AIA is committed to initiatives that secure information from cyber threats, and we continually work to encourage collaboration between industry and government on cybersecurity matters to include innovation, agility, and flexibility across all businesses and government entities supporting national and international missions.

**RE: FAR Case 2017-016: *Controlled Unclassified Information***

Thank you for the opportunity to provide these comments. Please direct any questions to Jason Timm, AIA's Senior Director, Security & Enterprise Management, at (703) 358-1043 or [jason.timm@aia-aerospace.org](mailto:jason.timm@aia-aerospace.org).

Sincerely,

A handwritten signature in black ink that reads "Margaret Boatner". The signature is written in a cursive style with a loop at the end of the last name.

Margaret Boatner  
Vice President, National Security Policy

Enclosure: AIA Comment Matrix – FAR Case 2017-016

| #             | From: | Type      | Starting Page # | Comment   | Suggested Change  |
|---------------|-------|-----------|-----------------|---|---|
| <b>Timing</b> |       |           |                 |   |   |
| 1             | AIA   | General   | 4297            | 52.204-VV Notice of Controlled Unclassified Information Requirements in paragraph (d) Unmarked CUI or mismarked CUI, requires Offerors to notify the Contracting Officer within 8 hours of discovery of any CUI not marked, not properly marked, not identified on the SF XXX form, or that is involved in a suspected or confirmed CUI incident.   | CMMC and DFARS 252.204-7012 require <b>incidents</b> to be reported in 72 hours. This requirement is not related to an "incident" and therefore is not time sensitive. Eight (8) hours is an unreasonably short time. <b>Recommend:</b> Since 32 CFR Part 2002 and NARA guidance requires the Government to mark information as CUI, contractors should not be made responsible for an inherently governmental function and do not have the authority to independently validate and mark Government's determinations. AIA recommends that to the extent contractors are required to notify the Government of potential marking issues, 10 working days should be sufficient to do so. |
| 2             | AIA   | General   | 4298 and 4299   | 52.204-XX Controlled Unclassified Information in paragraph (c)(1) outlines that the Contractor shall notify the Contracting Officer within 8 hours of discovery of: CUI not identified in the SF XXX or is not marked or properly marked, or there are inconsistencies. See also (g)(2)(ii) CUI Incidents - another reference to 8 hours. See also (h)(1)(iii) Subcontracts requirement to notify prime or next higher tier subcontractor within 8 hours of discovery of a suspected or confirmed CUI incident. | CMMC and DFARS 252.204-7012 require <b>incidents</b> to be reported in 72 hours. This requirement is not related to an "incident" and therefore is not time sensitive. Eight (8) hours is an unreasonably short time. <b>Recommend:</b> Since 32 CFR Part 2002 and NARA guidance requires the Government to mark information as CUI, contractors should not be made responsible for an inherently governmental function and do not have the authority to independently validate and mark Government's determinations. AIA recommends that to the extent contractors are required to notify the Government of potential marking issues, 10 working days should be sufficient to do so. |
| 3             | AIA   | General   | 4300            | 52.204-YY Identifying and Reporting Information That is Potentially Controlled Unclassified Information at paragraph (b)(1) stating the Contractor shall notify the Contracting Officer within 8 hours of discovery that the contractor believes, or has reason to know, is CUI. See also (e)(1) Subcontracts: Requiring subcontractors to report to the prime contractor or next higher tier subcontractor within 8 hours of discovery of a suspected or confirmed CUI incident.                               | CMMC and DFARS 252.204-7012 require <b>incidents</b> to be reported in 72 hours. This requirement is not related to an "incident" and therefore is not time sensitive. Eight (8) hours is an unreasonably short time. <b>Recommend:</b> Since 32 CFR Part 2002 and NARA guidance requires the Government to mark information as CUI, contractors should not be made responsible for an inherently governmental function and do not have the authority to independently validate and mark Government's determinations. AIA recommends that to the extent contractors are required to notify the Government of potential marking issues, 10 working days should be sufficient to do so. |
| 4             | AIA   | Technical | 11              | 8 hour requirement for notification of the Government does not align with other Government harmonization initiatives:<br>The requirement for contractors 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.  | CMMC and DFARS 252.204-7012 require <b>incidents</b> to be reported in 72 hours. This requirement is not related to an "incident" and therefore is not time sensitive. Eight (8) hours is an unreasonably short time. <b>Recommend:</b> Since 32 CFR Part 2002 and NARA guidance requires the Government to mark information as CUI, contractors should not be made responsible for an inherently governmental function and do not have the authority to independently validate and mark Government's determinations. AIA recommends that to the extent contractors are required to notify the Government of potential marking issues, 10 working days should be sufficient to do so. |
| 5             | AIA   | General   |                 | Identifying and reporting information the Contractor believes or has reason to know is potentially CUI:<br>The contractor shall notify the contracting officer within 8 hours if the contractor discovers any information that they believe is CUI but is not identified in the standard form SF-XXX or is not marked properly as required by the SF-XXX or there is any inconsistency between the clause (52.204-XX) and the standard form SF-XXX incorporated into the contract.                              | An 8-hour reporting timeline is insufficient for contractors to identify and report any information that they believe is CUI but is not identified, particularly when the CUI is not properly marked or identified. In such cases, contractors may require additional time to:<br>- Detect and verify the presence of CUI<br>- Assess the scope and severity of the incident<br>- Gather relevant information and evidence.   |

| #                  | From: | Type    | Starting Page # | Comment   | Suggested Change   |
|--------------------|-------|---------|-----------------|---|--|
| 6                  | AIA   | General |                 | <p>Assess and Report Suspected CUI Incidents:<br/>                     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 (<a href="https://dibnet.DOD.mil">https://dibnet.DOD.mil</a>) 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</p> | <p>The proposed 8-hour response time for confirmed or suspected CUI incidents is overly ambitious and may be unachievable. This truncated timeline does not provide sufficient time for the Incident Response Team and other stakeholders to conduct thorough investigations, gather necessary information, and take appropriate actions.<br/>                     Furthermore, this brief window may lead to an overwhelming workload for the team, stakeholders, and Points of Contact, potentially compromising the effectiveness of the response.<br/>                     Considering the DFARS requirement to report cyber-attacks within 72 hours of discovery: <b>Recommend</b> adopting a similar timeline for reporting CUI incidents. A 72-hour response window would provide a more realistic and manageable timeframe for responding to incidents, ensuring that all necessary steps are taken to contain and mitigate the incident.</p>  |
| <b>Definitions</b> |       |         |                 |   |  |
| 7                  | AIA   | General |                 | <p>Although 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 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 carveout for information a contractor possesses from non-Government sources or unrelated to Government contracts is not robust enough to preclude CUI requirements from being extended to such information. Specifically, contractor information merely possessed by the Government outside the scope of any Government contract is not included in a carveout and therefore 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 standard industry processes used to protect its own information.</p>   | <p><b>Recommend</b> the following changes to the definition of CUI under FAR 2.101, FAR 52.204-XX(a), and FAR 52.204-YY(a):<br/>                     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—<br/>                     (1) Classified information;<br/>                     (2) Covered Federal information (see 4.404-1);<br/>                     (3) Information a contractor possesses and maintains in its own systems that did not come from, or was not created <b>or possessed</b> by or <b>specifically</b> for, an executive branch agency or an entity acting for an agency (see 32 CFR 2002.4); <b>or</b><br/>                     (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; <b>or</b><br/>                     (5) <b>Technical data or computer software pertaining to commercial products or commercial services.</b></p> |
| 8                  | AIA   | General | 4298 and 4300   | <p>52.204-XX Controlled Unclassified Information at paragraph (c) "Identifying and reporting information the Contractor believes or has reason to know." How is "reason to know" to be defined or interpreted? Also appears in 52.204-YY Identifying and Reporting Information That is Potentially Controlled Unclassified Information at paragraph (b) and (b)(1).</p>   | <p>Recommend that "reason to know" is defined.</p>   |
| 9                  | AIA   | General | 4299            | <p>52.204-XX Controlled Unclassified Information at paragraph (h) Subcontracts: Subcontractors are to comply with the clause with no alteration except to identify the parties. Are one-time certifications enough?</p>   | <p>Recommend that the Government provide prime contractors with guidance for acceptable demonstrations of subcontractor compliance.</p>  |
| 10                 | AIA   | General | 4299            | <p>52.204-XX Controlled Unclassified Information at paragraph (g)(8): CUI Incidents: If a subcontractor fails to safeguard CUI, will the prime contractor be held fully responsible, even if the subcontractor was trained and the appropriate clauses were flowed down? Will there be any safe harbor provisions for primes that can demonstrate reasonable oversight?</p>   | <p>Recommend the Government provide examples of how prime contractors may demonstrate compliance and avoid liability when a subcontractor fails to safeguard CUI despite the existence of contractual flowdowns, training, and oversight.</p>  |

AIA Comment Matrix – FAR Case 2017-016

ENCLOSURE

| #  | From: | Type           | Starting Page # | Comment  | Suggested Change  |
|----|-------|----------------|-----------------|--|---|
| 11 | AIA   | General        | 4299            | 52.204-XX Controlled Unclassified Information at paragraph (f) Training requires general CUI training and points to the SF XXX form.   | Recommend the Government provide standardized training modules or certification programs that primes can use to ensure their own and subcontractor compliance. In the alternative, provide elements of satisfactory training so prime contractors can verify the adequacy of their own training programs and their subcontractor training programs.   |
| 12 | AIA   | Administrative | 10              | Clear guidance for "CUI Basic" and "CUI Specified":<br>The proposed use of the Standard Form (SF) XXX to communicate CUI could benefit from clear guidance differentiating between "CUI Basic" and "CUI Specified" and when each type is applicable in contracts.  | Include an appendix in the SF XXX form with examples of "CUI Basic" and "CUI Specified" scenarios for common use cases.   |
| 13 | AIA   | Technical      |                 | The rule identifies cloud computing services but not cloud service offerings which is the consistent way that other regulations identify non-providers   | Use standard terminology that is consistent with other regulations.   |
| 14 | AIA   | General        |                 | Definition of "discovery":<br>Clarify the definition of "discovery" that triggers the reporting requirements, particularly for cases of unmarked or mismarked CUI  | Highlight the importance of clearly defining "discovery." Provide reporting requirements  |
| 15 | AIA   | General        |                 | Determination of incident fault  | Request the removal of uncapped liability for government costs incurred in the response and mitigation effort if a contractor is determined to be at fault for an incident.<br><br>Uncapped liability for incident response under FAR Case 2017-016 is commercially unreasonable and imposes an undue financial burden on contractors, particularly small and mid-sized businesses. Even with robust cybersecurity measures, sophisticated cyber threats, including nation-state attacks, pose risks that no contractor can fully eliminate. Shifting unlimited financial responsibility onto contractors creates unpredictability, discourages participation in federal contracts, and undermines market stability. Instead, the government should implement a balanced approach, such as liability caps, cost-sharing mechanisms, or safe harbor protections for contractors demonstrating compliance with NIST SP 800-171 and other cybersecurity standards. Cybersecurity is a shared responsibility, and a collaborative risk model will better protect Controlled Unclassified Information (CUI) while maintaining a resilient and competitive defense industrial base. |
| 16 | AIA   | General        |                 | Definition of CUI Incident – “suspected or confirmed improper access, use, disclosure, modification, or destruction of CUI, in any form or medium.” This is broader than DFARS 252.204-7012 definition of “cyber incident”, because it focuses on the information and not just “computer networks”. However, the -7012 definition uses the phrase “actual or potentially adverse effect on . . . the information residing therein.”<br>What is the difference between “suspected” and “potentially”? | The DOD Cyber FAQ (Q:39) explains “An example of a potential adverse effect would be the discovery of malware on a contractor information system or network that was not blocked (e.g., by antivirus, or endpoint protection). In that case, malware was delivered via some mechanism and may or may not have affected covered defense information.”  |
| 17 | AIA   | General        |                 | CUI Incident Definon in FAR should clearly exclude unmarked or mismarked CUI where no mishandling or improper dissemination has occurred.  | While definition of a CUI Incident is quite broad, at multiple places within the specific regulations, it is repeatedly stated 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.   |
| 18 | AIA   | General        |                 | Definition of “Handling” – “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.”  | Because this definition includes the activities of collecting and developing, this arguably captures the concept of “CUI by compilation”. Define how a contractor is to know when collecting or developing information results in the creation of CUI.  |

AIA Comment Matrix – FAR Case 2017-016

ENCLOSURE

| #                        | From: | Type      | Starting Page # | Comment  | Suggested Change  |
|--------------------------|-------|-----------|-----------------|--|---|
| 19                       | AIA   | General   |                 | Covered Federal Information – This is the same definition as Federal Contract Information. However, that definition includes the phrase “simple transactional information (such as that necessary to process payments”.  | This has caused confusion for years, particularly among finance departments who have often asked whether sales quotes, invoices for products/services, and internal spreadsheets are FCI (now CFI). Also, the proposed rule states “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.” This means that some CFI will be marked, while some won’t, making things worse. |
| <b>NIST Standards</b>    |       |           |                 |  |   |
| 20                       | AIA   | General   | 31              | NIST SP 800-171 R3   | FAR CUI-48CFR references NIST SP 800-171 extensively with no reference to when/how/if R3 will be implemented.   |
| 21                       | AIA   | General   | 22              | CUI Identified During Solicitation Phase:<br>"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."                        | If contractors are required to identify unmarked CUI during the solicitation process of a bid/contract proposal, how are they held liable for unmarked CUI? How does this apply to the 8 hour rule on p25, 33, 75, etc.   |
| 22                       | AIA   | Editorial |                 | Lack of harmonization with all other recent regulatory requirements related to incident reporting, CUI, and NIST SP 800-171/800-172  | Read all of the recent comments for all regulations related to CUI and incident reporting such as the CMMC Rule (32 CFR Part 170, 48 CFR Parts 204, 252, CIRCIA, etc.) to understand concerns and challenges already addressed and identified by industry.  |
| 23                       | AIA   | General   |                 | NIST 800-172 requirements:<br>The NIST 800-172 requirements in the appendix differ from those the Defense Industrial Base was worked with DOD to identify for CMMC Level 3.  | This is a step backwards from the progress that's been made.  |
| 24                       | AIA   | Technical |                 | What about other types of service providers other than cloud?  | There should be information about how other service providers (non-CSP) as well as other cloud offerings.   |
| 25                       | AIA   | General   |                 | There is a major disconnect on costs for NIST SP 800-172 between this rule and others such as in CMMC FAR 32CFR rule:<br>The cost estimate for implementing NIST SP 800-172 is identified as \$202,500 with 20% annual recurring but the CMMC FAR CUI Rule Part 170 identifies the implementation of NIST SP 800-172 as either \$21,100,000 for implementation and \$4,120,000 recurring for other than smalls and \$2,700,000 for implementation and \$490,000 for recurring costs for small businesses. This is a 10 or 100 times difference in estimates. | Make consistent cost estimates that are more realistic and consistent with other cost assessments.  |
| <b>FAR CUI Questions</b> |       |           |                 |  |   |
| 26                       | AIA   | General   |                 | FAR CUI Question #1:<br>Is there additional information or guidance you view as necessary to effectively comply with this rule?  | More information needs to be provided as part of the rule including definitions and details on missing aspects such as how service providers are part of the rule and how the data will be stored for contracts identifying CUI so minimize constant back and forth requests to determine if something is or is not CUI.<br><br>Recommend coordinating with DOD to align the definition of CDI in DFARS 252.204-7012 to eliminate confusion as to whether CDI is the same as CUI or whether it is more expansive or restrictive.  |



| #                             | From: | Type      | Starting Page #      | Comment  | Suggested Change   |
|-------------------------------|-------|-----------|----------------------|--|--|
| 27                            | AIA   | General   |                      | FAR CUI Question #2:<br>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?  | Yes. Incident response timelines are different than other regulatory requirements such as with the DOD and DHS. The additional administrative overhead for managing different timelines will require additional costs and resources for the administrative work above and beyond the incident management resources to resolve the incidents.<br><br>Recommend aligning to the DOD's 72 hour requirement. |
| 28                            | AIA   | General   |                      | FAR CUI Question #3:<br>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?  | The implications are that additional resources will be required since many of the incidents would need to be handled by others to resolve incidents in a timely manner. Additionally, reporting and handling "possible" CUI incidents as another level of administrative overhead that cannot be truly understood without additional data and details.   |
| 29                            | AIA   | General   |                      | FAR CUI Question #4:<br>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?  | The initial costs would be at least 2-3 times more per incident and could be 2-10 times more incidents if "suspected" or "potential" incidents are required to be reported.<br><br>Is this the cost of responding to an incident or the cost of the product? The questions asks about the cost of product. Can someone in business management help with an estimate?                                     |
| 30                            | AIA   | General   |                      | FAR CUI Question #5:<br>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.  | Managing data is hard enough currently, especially when trying to work with a disparate and multi-level supply chain. Without adequate management of the data for a program that can be easily stored and accessed to identify whether data has been deemed CUI or not will be necessary to manage the administrative overhead of multiple levels of requests.   |
| 31                            | AIA   | General   |                      | FAR CUI Question #6:<br>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. | CUI should be handled as CUI and anything that is CUI Specified should be called out specifically in the contract and handled accordingly without the need to add more overhead to this rule. However, the processes and procedures for properly identifying this data should be in the rule as well.<br><br>The Government needs to use limited dissemination control markings.                         |
| <b>Other General comments</b> |       |           |                      |  |  |
| 32                            | AIA   | General   |                      | Concerns about the rule's lack of consideration for external service providers, such as managed service providers (MSPs)   | Provide examples of how incidents on MSPs can impact the primary contractor's CUI environment, highlighting the need for clear reporting requirements  |
| 33                            | AIA   | Editorial |                      | The forms for CUI do not address the challenges with FCI   | Modify the forms to also identify FCI on the contract to allow for understanding and providing adequate protections per other FAR rules  |
| 34                            | AIA   | General   |                      | Flowdown   | Request requirement for the Prime contractors to accurately identify the CUI subcontractors will handle by providing or utilizing the same description as provided in the SF-XXX.  |
| 35                            | AIA   | General   | 4281<br>4298<br>4300 | Unclear and contradictory context regarding confusing statements in the proposed rule that say the contractor is "not permitted to use Government-provided information for its own purposes."  | Recommend clarification for several confusing statements in the proposed rule that say the contractor is "not permitted to use Government-provided information for its own purposes." The context is unclear and is contradictory. Page 4281, page 4298 para (c)((4), and page 4300 para (c).  |
| 36                            | AIA   | General   |                      | There doesn't seem to be a process of how to decouple or deaggregate the information to move from CUI to FCI and/or neither.   | Provide a process, guidance, and documentation for how to move CUI information to non-CUI so that flowdowns can appropriately and adequately applied to subcontractors throughout the supply chain.  |

| #  | From: | Type      | Starting Page # | Comment   | Suggested Change   |
|----|-------|-----------|-----------------|---|--|
| 37 | AIA   | Technical |                 | Tracking of CUI via paper and forms is not efficient or effective.  | There should be a database and tracking for data and its categorization to minimize administrative impacts on responding to "suspected" CUI.   |
| 38 | AIA   | General   |                 | Disparate incident reporting requirements:<br>The creation of disparate incident reporting requirements as each contract will have a separate Standard Form identifying these requirements.   | This will be tough to track and should go to a central location.<br><br>Requiring contractors to report CUI incidents separately to each contracting agency creates unnecessary duplication, administrative burden, and potential inconsistencies in incident response. A decentralized reporting approach strains contractor resources, delays response efforts, and increases the risk of fragmented or incomplete information reaching the appropriate government stakeholders. Instead, a centralized CUI incident reporting system within the U.S. government—such as a designated agency or cybersecurity office—would streamline reporting, enhance coordination, and ensure timely and consistent threat analysis across federal contracts. This approach would improve national security by allowing the government to aggregate threat intelligence, identify patterns, and respond more effectively to emerging cyber threats while reducing unnecessary burdens on contractors.  |
| 39 | AIA   | General   |                 | Responsibility of CUI incident response costs - Contractors “may be financially liable” for the Government’s response costs “in addition to any other damages at law or remedies available to the Government for noncompliance” if the contractor “is determined to be at fault for a CUI incident.”  | The proposed rule does not specify how the Government would pursue such a claim, but it’s likely that the contracting officer would have to do so on behalf of the Government under the Contract Disputes Act.<br><br>Uncapped liability for incident response under FAR Case 2017-016 is commercially unreasonable and imposes an undue financial burden on contractors, particularly small and mid-sized businesses. Even with robust cybersecurity measures, sophisticated cyber threats, including nation-state attacks, pose risks that no contractor can fully eliminate. Shifting unlimited financial responsibility onto contractors creates unpredictability, discourages participation in federal contracts, and undermines market stability. Instead, the government should implement a balanced approach, such as liability caps, cost-sharing mechanisms, or safe harbor protections for contractors demonstrating compliance with NIST SP 800-171 and other cybersecurity standards. Cybersecurity is a shared responsibility, and a collaborative risk model will better protect Controlled Unclassified Information (CUI) while maintaining a resilient and competitive defense industrial base. |
| 40 | AIA   | General   |                 | Disclosure, protection, and marking of contractor information. “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. . . . 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. . . . (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.” | Seems like the contracting officer gets the final word, even if the contractor disagrees. What is the mechanism for appeal (i.e., to the Agency CUI office, Agency Head, etc...)?  |

AIA Comment Matrix – FAR Case 2017-016

ENCLOSURE

| #  | From: | Type    | Starting Page # | Comment  | Suggested Change  |
|----|-------|---------|-----------------|--|---|
| 41 | AIA   | General |                 | <p>Application of CUI Requirements to Commercial Products and Commercial Services. Although the FAR proposed language has a distinct carveout for data associated with Commercial Off the Shelf (COTS) Items, the language contradictorily states that CUI requires protection regardless of dollar value or commerciality of the product or service so the rule also applies to contracts at or below the simplified acquisition threshold (SAT) and to commercial products and commercial services. Instead of making an artificial distinction between commercial items 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 generally. COTS items can also come with proprietary supplier data. If the Government’s interest is required 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. 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 loss of contractors willing to do business with the Government and ultimately an increase of costs of Government procurement with little benefit or loss of available technologies.</p> | <p>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 services so they can continue to implement their own best practices for protecting their own proprietary information.</p>   |
| 42 | AIA   | General |                 | <p>Unmarked or mismarked CUI – “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.”</p>   | <p>The statement has circular logic because it defines a CUI incident as a situation where the mishandling or improper dissemination of CUI has occurred, but then it also implies that the mishandling or improper dissemination of CUI is a result of the mismarking or lack of marking of CUI in the first place. In other words, the statement is saying that a CUI incident occurs when CUI is mishandled or improperly disseminated, but then it’s also saying that the mismarking or lack of marking of CUI is what caused the mishandling or improper dissemination of CUI. This creates a circular definition, where the cause (mismarking or lack of marking) is being used to define the effect (mishandling or improper dissemination). To break the circular logic, the statement could be rephrased to say something like: "Mismarking or lack of marking of CUI can lead to a CUI incident if it results in the mishandling or improper dissemination of the information." This revised statement avoids the circular definition and provides a clearer explanation of the relationship between mismarking or lack of marking and CUI incidents.</p> <p>Since 32 CFR Part 2002 and NARA guidance requires the Government to mark information as CUI, contractors should not be made responsible for an inherently governmental function and do not have the authority to independently validate and mark Government’s determinations. To the extent the Government’s failure to properly mark information as CUI results in an incident, the contractor should not have any liability.</p> |

AIA Comment Matrix – FAR Case 2017-016

ENCLOSURE

| #  | From: | Type    | Starting Page # | Comment  | Suggested Change   |
|----|-------|---------|-----------------|--|--|
| 43 | AIA   | General |                 | Agencies can add more requirements for their CUI – “(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.” See also “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).”  | If agencies can add more requirements for their CUI – but those requirements are not for handling CUI Specified or imposing NIST SP 800-172 enhanced controls, this can create confusion.  |
| 44 | AIA   | General |                 | FedRAMP Moderate – “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 ( <a href="https://www.fedramp.gov/documents/">https://www.fedramp.gov/documents/</a> ).”:<br><br>This differs from DFARS 252.204-7012 “If the Contractor intends to use an external cloud service provider to store, process, or transmit any covered defense information in performance of this contract, the Contractor shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline ( <a href="https://www.fedramp.gov/documents-templates/">https://www.fedramp.gov/documents-templates/</a> ) and that the cloud service provider complies with requirements in paragraphs (c) through (g) of this clause for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment.” | While the proposed FAR rule removes the word “equivalent”, it does not clarify whether cloud providers can have POA&Ms (DOD does not allow them, though they are allowed if the cloud provider has an ATO (memo doesn’t apply) or has inherited the POA&Ms from an IaaS provider (official, but not in memo)). Also, does the cloud provider have an obligation to comply with the CUI incident reporting requirements?<br><br>It is evident this is being interpreted differently by different people, and so clarity around FedRAMP requirements is definitely needed.   |
| 45 | AIA   | General |                 | Potential exposure of proprietary information to competitors – “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.”   | A contractors competitors would have access to sensitive cybersecurity information, which we already refuse to provide through cybersecurity questionnaires.<br><br>Third parties often have their own agendas and conflicts of interest. The requirement for third parties to have broad access to contractors information systems has caused problems for DIB companies.   |
| 46 | AIA   | General |                 | Comments regarding the SF XXX:<br>We really like the idea of an SF XXX that will tell us about the type of CUI we will be working with   | The rule could go further in at least one area. It seems it doesn’t discuss how to determine that the specific information, brief, paper, etc., we are working on/creating is CUI and what category of CUI it is. It is great that industry may have multiple categories that may be on the contract, but it doesn’t connect all the dots. Does industry assume that everything it generates under a contract with the SF XXX is CUI and all the categories listed there? It may be agreeable in some cases, it may be easy to tell a difference (e.g., Financial information vs. water assessments), but others may be more difficult (Export Controlled vs. Controlled Technical Information). To better determine applicability, industry needs something like a security classification guide to connect these dots. |

| #  | From: | Type    | Starting Page # | Comment   | Suggested Change  |
|----|-------|---------|-----------------|---|---|
| 47 | AIA   | General |                 | <p>Comments regarding the SF XXX:<br/>                     The variation in how SF XXX might be filled out by different Contracting Officers means we may have varying levels of training, policies, handling requirements for each different contract.</p>   | <p>The following verbiage lends itself to variations in each contract we receive:<br/>                     "comply with the requirements identified in Part C of SF XXX<br/>                     "unless the employee has completed training on properly handling CUI that, at a minimum, includes the elements required in the SF XXX"<br/>                     "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;"<br/>                     "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."<br/>                     Report incidents "to the agency website or single point of contact identified in Part C, Section IV of the SF XXX;". This could end up being a different POC for every contract we have.</p> |
| 48 | AIA   | General |                 | <p>Some confusing/conflicting statements could use clarity.</p>   | <ol style="list-style-type: none"> <li>1. 4.403-4(c) says that “Offerors and contractors are not responsible for identifying or marking unmarked or mismarked CUI that is not identified in the SF XXX”</li> <li>2. 52.204-WW(d): “ The contractor is required to safeguard only the CUI identified in the SF XXX. However, see paragraph (c)(2) of this clause.” (emphasis ours)</li> <li>3. (c)(2) of this clause says almost the exact opposite of the guidance provided in the above to references saying we are required to safeguard other CUI. In reality, we are required to safeguard anything we suspect is CUI whether it is marked, mismarked or not identified in the SF XXX.</li> </ol>   |
| 49 | AIA   | General |                 | <p>Safeguarding CUI:<br/>                     (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</p>   | <p>The provision's lack of a specified cap on financial liability poses a significant risk to contractors, potentially leading to catastrophic financial consequences.</p> <ul style="list-style-type: none"> <li>-Establish a clear cap on financial liability to protect contractors from excessive costs.</li> <li>-Specify the types of incidents that would trigger financial liability, ensuring clarity and consistency.</li> <li>-Define the circumstances under which the Government would assume responsibility for incident response and resolution.</li> <li>- Establish clear guidelines on the extent to which contractors are expected to resolve incidents independently before reporting to the Government.</li> </ul>   |
| 50 | AIA   | General |                 | <p>Train Employees on Handling CUI:<br/>                     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.<br/>                     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.</p> | <p>Recommend that the Government provide standardized safeguarding CUI training to all contractors, similar to the marking of CUI training. This uniform training approach would ensure consistency and accuracy in CUI handling across all contractors.<br/>                     Additionally, providing government-led training would alleviate a significant financial burden on contractors. Currently, contractors would need to invest substantial resources in developing and delivering their own training programs, hiring additional personnel, or providing training to existing personnel.</p> <p>By providing centralized training, the Government can:</p> <ul style="list-style-type: none"> <li>- Ensure uniformity and consistency in CUI handling</li> <li>- Reduce the financial burden on contractors</li> <li>- Enhance overall CUI security and compliance</li> </ul>   |

| #  | From: | Type    | Starting Page # | Comment   | Suggested Change   |
|----|-------|---------|-----------------|---|--|
| 51 | AIA   | General |                 | <p>Compliance:<br/>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.</p>   | <ol style="list-style-type: none"> <li>1. Who will conduct the validation actions? Will it be Government officials, a Certified Third-Party Assessment Organization (C3PAO), or another entity?</li> <li>2. What are the criteria for selecting systems for validation? Will it be based on risk assessments, system criticality, or other factors?</li> <li>3. Under what conditions will validation actions be performed? Will it be triggered by specific events, such as incidents or changes to the system?</li> <li>4. Will validation actions be performed randomly or on a scheduled basis? If random, how will the selection process ensure fairness and equity?</li> <li>5. How will the agency determine which non-Federal information systems are applicable? What criteria will be used to define the scope of applicable systems?</li> </ol> |
| 52 | AIA   | General |                 | <p>Policy:<br/>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.</p>   | <p>To ensure clarity and precision, it is strongly recommended that the SF XXX include an itemized list or explicit identification of Controlled Unclassified Information (CUI) requirements. This would prevent potential issues where a contracting officer defines a broad category of CUI without providing specific details, leading to confusion and ambiguity. By providing a clear and detailed list of CUI requirements, contractors can better understand their obligations and ensure compliance with the relevant regulations and standards</p>  |
| 53 | AIA   | General |                 | <p>Policy. Of note, correctly identifying, defining, marking and delivering information as CUI is an inherently governmental function. It is imperative that we are careful about the FAR levying protection/marketing requirements to force contractors to broadly label and protect their own information as CUI to meet a government protection requirement before providing it to the Government. Such requirements would ultimately drive unnecessary cost and complexity into doing business with the Government resulting in further erosion of the Government contracting industrial complex.</p>   | <p>To help alleviate concerns, the CUI definition is proposed to be modified (see comment #7 above) to provide a clear boundary to the marking requirements extents possible in the SF XXX.</p>  |
| 54 | AIA   | General |                 | <p>Scope of Requirements to Patent Applications. The FAR proposed rule includes language requiring protection of patent applications as CUI. While it is understandable that the Government wants to safeguard patent applications when handling an unpublished or draft patent application, it must be careful about the updated FAR 27.203-1 imposing additional requirements on contractor/inventor protection of patent applications and patent-related materials once they are designated as CUI. If this becomes the case, there are widespread ramifications that are especially highlighted in areas where research is being conducted without significant capital resources or information security infrastructure. For example, small businesses filing patent applications may not have sufficient facility protections, information security protections, or resources, and may be forced to upgrade their equipment and systems simply because they seek to protect their own innovations developed under SBIR/STTR programs. These additional requirements may ultimately encourage small businesses to not file on their innovations, not securing the Government’s investment in such entities, or even chill small business participation in SBIR/STTR programs.</p> | <p>Patent applications should be carved out from the definition of CUI.</p>  |