February 2, 2024

William F. Clark
Director, Office of Government-wide Acquisition Policy
General Services Administration
1800 F Street NW
Washington, DC 20405

VIA ELECTRONIC SUBMISSION

Re: Comments in response to FAR Case 2021-017

Dear Mr. Clark:

The Cybersecurity Coalition ("Coalition") and the Alliance for Digital Innovation (ADI) appreciate the opportunity to submit comments to the Department of Defense (DOD), General Services Administration (GSA), and National Aeronautics and Space Administration (NASA) regarding our concerns with Federal Acquisition Regulation (FAR) Case 2021-017. We understand that this proposed rule has been created to fulfill a direct requirement from the Executive Order (EO) on Improving the Nation's Cybersecurity (EO 14028). As such, we would expect the requirements in this FAR case to be closely aligned with requirements of EO 14028. We hope that our comments will lead to further clarification and revision of the proposed rules so that industry may effectively comply with new cyber threat reporting and information sharing requirements.

The Coalition is composed of leading companies specializing in cybersecurity products and services dedicated to finding and advancing consensus policy solutions that promote the development and adoption of cybersecurity technologies. We seek to ensure a robust marketplace that will encourage companies of all sizes to take steps to improve their cybersecurity risk management. We are supportive of efforts to identify and promote the adoption of cybersecurity best practices, information sharing, and voluntary standards throughout the global community.

ADI is a non-partisan alliance that advocates for the removal of institutional and bureaucratic barriers to the operation of a modern digital government. Our members provide key critical technologies to the Government, including cloud infrastructure, digital identity solutions, human resources software, quantum computing, digital services, and a range of sophisticated cybersecurity tools and services. We support the adoption of innovative commercial technologies by the Federal Government.

Section I - Summary of Issues

Before answering the specific questions detailed within the proposed rule, the Coalition and ADI would encourage the Government to consider following:

1. **Industry and government are not the same.** When creating cybersecurity requirements, the Government should not attempt to hold federal contractors and industry to the same standards as it would federal agencies. Whereas federal agencies face few consequences if they fail to meet *Federal Information Security Modernization Act* (FISMA) requirements, federal contractors and industry may face criminal prosecution if they violate FAR clauses. Therefore, the Government must make FAR clauses pragmatic rather than aspirational. If not, the Government could unintentionally shrink the market of available federal contractors and limit its ability to leverage innovative technologies and solutions.

2. **SBOMs are still being conceptually developed.** EO 14028 highlights the potential value that Software Bills of Materials (SBOMs) can provide to both producers and consumers of software solutions. The Coalition and ADI support the vision for SBOMs established in the EO and believe there is significant work to be done to achieve it. Indeed, SBOMs are not yet commonplace in the vast majority of delivered software and are not standardized in policy or technical circles. This is especially true of SBOMs for cloud and hybrid products, which have a unique set of implementation challenges. Therefore, the Coalition and ADI recommend that the Government encourage, but not require, federal contractors to provide SBOMs for cloud and hybrid products. We also urge the Government to adopt a deliberate and collaborative approach to creating SBOM requirements for on-premises products.

3. **Providing "full access" to contractor systems is unprecedented.** The proposed rule would provide federal agencies with "full access" to a federal contractor's IT systems following a cybersecurity incident. According to the current language of the proposed rule, this full access would be unbounded and would allow the Government to have an unprecedent degree of access to information about the federal contractor, its employees, its business systems, and potentially its non-federal clients. Furthermore, this requirement could expose some federal contractors to breach of contract claims from their non-federal customers. It is unreasonable to require a federal contractor to provide this degree of access to information simply because it is selling to the Government. Additionally, the requirements for access outlined in the proposed rule are not aligned with any requirements from EO 14028. The EO appropriately directs the creation of a rule that requires federal contractors to share relevant information and collaborate with federal cybersecurity or investigative agencies on incidents. We encourage the establishment of requirements that are aligned with EO 14028 rather than the current provisions that will discourage contractors from seeking to deliver services to the federal ecosystem.

4. **Incident reporting requirements should be reasonable and harmonized.** The proposed rule would tie incident reporting timelines to the identification that a security incident may have occurred rather than to a determination an incident has occurred. The proposed eight-hour reporting timeline combined with requirement to report when an incident may have occurred would result in the reporting numerous false positives. This would, in turn, increase costs for both federal contractors and the Government. Given the number of cyber-attacks all organizations experience, it is more appropriate to allow time for investigation in advance of reporting. This problem is only exacerbated by the fact that federal contractors must follow numerous other disparate federal reporting requirements. We encourage the creation of a rule that is modeled after the *Cyber Incident Reporting for Critical Infrastructure Act* (CIRCIA), which has a reporting timeline that begins when an organization determines that an incident has occurred. At the very least, the proposed rule should establish a reporting timeline based on

when the federal contractor should reasonably determine that an incident likely occurred. This will allow companies to focus on incident response during the critical early stages of a cyber-attack rather than compliance and reporting activities.

5. **Increased regulatory burden blocks small businesses.** By creating increasingly complicated requirements for cybersecurity, the Government would increase the cost of compliance for federal contractors. These burdens would limit the number of small businesses interested in providing services to the Government.

Section II - Question Responses

Below, the Coalition and ADI provide responses to the specific questions posed in FAR Case 2021-017 and additional recommendations for the final rule:

II. Discussion and Analysis – *a. Software Bills of Materials*

Question 1: *How should SBOMs be collected from contractors? What specific protections are necessary for the information contained within an SBOM?* The Coalition and ADI believe that SBOMs are not yet fully developed and that overly strict requirements them could harm their adoption. Therefore, we recommend that the Government adopt a collaborative approach to SBOMs that works with industry to improve their efficacy and facilitate their adoption.

The Coalition and ADI believe that the Government should not require SBOMs for cloud service products. Cloud Service Providers (CSPs) frequently change their products, using the information an SBOM would contain to apply security updates on behalf of users (i.e., on behalf of the Government). Instead, the Coalition and ADI suggest that the Government allow CSPs to demonstrate their maintenance of software provenance information through verification with a 3PAO under the FedRAMP program.

For the SBOMs and other artifacts (e.g., class diagrams, risk assessments, etc.) the Government does collect from federal contractors, the Coalition and ADI believe the Government should implement the following protective measures:

- Use secure, digital channels (e.g., Digital Bill of Materials (DBoM) or secure Application Programming Interface (API) calls) to collect all artifacts.

- Adopt a Digital Rights Management approach that protects SBOMs based on their level of sensitivity. Within this approach, the Government should create access controls that prevent unauthorized viewing of artifacts. Access to SBOMS should be limited to CISA and the agency who has contracted with the vendor supplying the SBOM. SBOMs should not be widely available to all Government organizations.

- Prevent the access of SBOMs and other artifacts through Freedom of Information Act (FOIA) Requests. To accomplish this, the Government should specify in Case 2021-017 that SBOMs receive protections under FOIA Exemption 4: "[t]rade secrets or commercial or financial information that is confidential or privileged."[i] Subsequently, federal contractors could indicate in their submissions when they believe FOIA Exemption 4 applies to an artifact.

Question 2: *How should the Government think about the appropriate scope of the requirement on contractors to provide SBOMs that ensure appropriate security?*

As stated in NTIA's July 2021 SBOM Minimum Elements Report, "an SBOM provides those who produce, purchase, and operate software with information that enhances their understanding of the supply chain, which enables multiple benefits, most notably the potential to track known and newly emerged vulnerabilities and risks."[ii] Thus, SBOMs on their own do not "ensure appropriate security," but rather are a tool network defenders can use to better understand their organization's operating environment.

Since SBOMs contain information that could identify potential vulnerabilities, they pose a risk if exposed. For example, SBOMs give malicious actors significant information to help direct their vulnerability discovery efforts. This risk is magnified if multiple SBOMs are centrally located in a repository that does not have sufficient technical safeguards. Moreover, this risk is magnified for Cloud service Providers (CSPs), which have multiple customers connected to product instances. Therefore, the Coalition and ADI recommend that the Government carefully consider whether it desires to hold this SBOM information. If the Government decides that it does want this information, it should only require SBOMs for on-premises software. It must also, at a minimum, provide proper access controls, implement encryption at rest, and assume liability if a disclosure to non-authorized actors causes harm to the SBOM provider.

Question 3: *What challenges will contractors face in the development of SBOMs? What challenges are unique to software resellers? What challenges exist regarding legacy software?*

Third-Party Resellers – The Coalition and ADI would first highlight that a plurality of federal contractors providing software to the Government are third-party resellers, are ***not*** original publishers. Therefore, the following challenges should be treated as core issues, not edge cases:

- Since third-party resellers do not develop or maintain software themselves, they rely on original publishers to create SBOMs on their behalf. Meanwhile, FAR Case 2021-017 states that federal contractors must "develop and maintain a software bill of materials (SBOM) for any software used in the performance of the contract." This means a third-party reseller could theoretically be held liable for breach of contract if the original publisher fails to "develop and maintain" an SBOM. Therefore, the Coalition and ADI recommend that the Government specify that federal contractors "***make a good faith effort*** to develop and maintain [SBOMs] for any software used in the performance of the contract."

- Multiple third-party resellers and original publishers may all provide the same software to the Government through different contracts. Depending on the end requirements of the contract, each reseller and publisher may produce slightly different SBOMS depending on the tool used. This raises questions over whether a federal contractor could be held liable for providing insufficient SBOMs if another federal contractor provides a more detailed one. Therefore, the Coalition and ADI recommend that the Government explicitly state that SBOMs for the same product provided by different contractors do not need to be identical.

Legacy Products – In the future, the Government may still need to procure legacy solutions for which a federal contractor has not developed an SBOM. This could cause a situation where the proposed FAR rules prevent the Government from procuring legacy software for which no

SBOM exists. The Coalition and ADI suggest that the Government base SBOM requirements on the procured software's date of development rather than its date of purchase.

Cloud Products – As discussed in NTIA's July 2021 SBOM Minimum Elements Report, cloud products and Software-as-a-Service (SaaS) have unique challenges with respect to SBOMs.[iii] In comparison to on-premises software, SaaS updates are made far more frequently and have incremental changes. Using current methods of SBOM creation, it would be incredibly burdensome - or in some cases impossible - for federal contractors providing SaaS solutions to maintain fully accurate SBOMs. Therefore, the Coalition and ADI recommend that the Government only require SBOMs for on-premises software solutions. Rather than collect SBOMs for cloud service offerings, we recommend that the government allow CSPs to work with their FedRAMP 3PAOs to verify that they maintain software provenance data. In this instance, the Government's role would be to regularly verify that these systems and processes are in place through the FedRAMP Program.

Question 4: *What are the appropriate means of evaluating when an SBOM must be updated based on changes in a new build or major release?*

The Coalition and ADI believe that the Government should require SBOM updates after a major release or when the federal contractor updates existing dependencies or includes new dependencies. To improve clarity, the Government should also encourage federal contractors to align their software release version numbers with their SBOM version numbers.

Question 5: *What is the appropriate balance between the Government and the contractor, when monitoring SBOMs for embedded software vulnerabilities as they are discovered?*

As software producers become aware of new vulnerabilities, it is incumbent upon them to notify their customers (including the Government), of vulnerabilities and issue software updates when appropriate. However, in practice, software producers are often not aware of the operational environment in which their federal customers are using their products. Therefore, it is also incumbent upon the Government to track vulnerabilities to their systems – including those found in SBOMs – and implement suitable mitigations. For this to be effective, Government customers must update its software and apply recommended configuration changes where possible.

To broadly improve vulnerability management, the Coalition and ADI recommend that the Government require all federal contractors and software producers to implement Vulnerability Disclosure Programs (VDPs)as part of their overall risk management programs. Additionally, we urge the Government to focus its SBOM monitoring efforts on finding vulnerabilities that can be activated or exploited. Specifically, the Government should check SBOMs for vulnerabilities in CISA's Known Exploited Vulnerabilities (KEV) Catalog, which records all vulnerabilities exploited in the wild.

II. Discussion and Analysis – *b. Access to Contractor Information and Information Systems*

Question 1: *Do you have any specific concerns with providing CISA, the FBI, or the [contracting] agency full access (see definition at 52.239–ZZ(a)) information, equipment, and to contractor personnel? Please provide specific details regarding any concerns associated with providing such access.*

The Coalition and ADI believe that the scope of the term "full access" in 52.239–ZZ is unbounded and could allow the Government to access any part of a federal contractor's systems. Clause 52.239–ZZ(a) defines "full access" as including access to Government systems, "other infrastructure housed on the same computer network," and "other infrastructure with a shared identity boundary or interconnection to the Government system." This definition would provide the Government with an unprecedented degree of access to federal contractors' systems and raises questions as to what types of systems may not be subject to federal access during an investigation into a cybersecurity incident.

The Coalition and ADI would also highlight that, in most instances, federal contractors also conduct business with non-federal clients. These clients may become concerned that the FAR rules now allow the Government to access their data without any due process. Consequently, non-federal clients may decide to no longer do business with the federal contractor. This could force the federal contractor to either lose out on its non-federal business or decide to no longer provide services to the Government.

The Coalition and ADI believe that the proposed rule significantly exceeds EO 14028's direction to create a rule that requires federal contractors to collect and preserve data, share data and information related to cyber incidents, and collaborate with federal cybersecurity and investigative agencies in response to an incident. The Coalition and ADI recommend that the Government develop rules that adhere to the requirements established in EO 14028.

If the Government is insistent on including a provision that would allow access to a federal contractor's system, then the Government must define specific criteria for what triggers its ability to enter it. In the proposal, clause 52.239–ZZ (c)(6)(i) states that the Contracting Officer, CISA, or the FBI may request access to any "information or equipment that is necessary to conduct a forensic analysis" in response to "an identified security incident." Upon request, the federal contractor must provide the information or equipment within 96 hours. According to this language, the Government may request access after any security incident it chooses, regardless of severity.

Question 2: *For any specific concerns identified, are there any specific safeguards, including safeguards that would address the scope of full access or how full access would be provided, that would address your concerns while still providing the Government with appropriate access to conduct necessary forensic analysis regarding security incidents?*

To address this problem, the Coalition and ADI urge the Government to eliminate the "full access" provision in clause 52.239–ZZ(c)(6)(i) of the proposed rule. Instead, the Government should add language requiring federal contractors to collaborate with cybersecurity and investigative agencies (i.e., CISA and the FBI) in response to an incident. The Government could also require that federal contractors provide certain information or updates when government information is implicated in the incident.

However, if the Government insists on gaining "full access" to federal contractor systems, the Coalition and ADI suggest that the Government:

- Create an escalations process that would allow the Government to access a federal contractor's systems and personnel *only if* the federal contractor is not being responsive to or cooperative with the Government's investigation.

- Establish criteria that would only allow access to federal contractor systems for incidents that are determined to be "significant cyber incidents" under the definition established in Presidential Policy Directive 41.[iv]

- Create an appeals mechanism for federal contractors to contest the Government's access and entry into their IT systems. Preemptively, this mechanism would allow federal contractors to prevent access to their systems and information if it is unnecessary.

- Restrict the scope of the Government's access to only include federal contractor systems that either contain or are involved in the protection of Government or Government related data. As explained in our response to Question 1 of this section, the current language of the proposed rules could allow the Government to access systems belonging to a federal contractor's non-federal clients. To prevent the Government from accessing these private systems, the FAR rules should specify that the Government may only access systems which the federal contractor has identified as containing Government information or directly supporting the delivery of the terms of the contract. To accomplish this, the Government could redefine "full access" in clause 52.239–ZZ(a) so that is has the following meaning:

    - "*Full access* means, for all contractor information systems used in performance of the contract — (1) Electronic access to— (i) Contractor networks *that are dedicated to Government data*, (ii) Systems, (iii) Accounts dedicated to Government systems *only*, (iv) Other infrastructure with a shared identity boundary or interconnection to the Government system; and (2) Provision of all requested Government data or Government-related data, including— (i) Images, (ii) Log files, (iii) Event information.

- Establish limitations and safeguards for the information that the Government accesses and collects from federal contractor systems. Specifically, the Government should ensure that the information it collects retain their original legal privileges and protections (e.g., trade secrets, employee data, attorney-client privilege, etc.). The Government should also refrain from accessing and collecting information that it cannot procedurally or technically protect (e.g., attorney client privileged information, which could be accessed via a FOIA request). To clearly define what it has the right to access, the Government should also redefine "Government-related data" in clause 52.239–ZZ(a) so that it has the following meaning:

    - "*Government-related data* means any information, document, media, or machine-readable material regardless of physical form or characteristics that is created or obtained by a contractor through the storage, processing, or communication of Government data. Government-related data does not include— (1) A contractor's business records *and other contractor privileged and confidential information* (*e.g.,* financial records, legal records) that do not incorporate Government data; or (2) Data such as operating procedures, *software coding or algorithms, operating procedures, software coding or algorithms that do not incorporate Government data.* (3) Data or meta-data related to the security, performance or features of the contractor's service. This information may be used by the contractor to identify and implement product enhancements, including those aimed at improving the security of the broader ecosystem."

Question 3: *Subparagraph (g)(i)(C) of section 2 of E.O. 14028 recognizes the need to identify appropriate and effective protections for privacy and civil liberties. Are there any specific safeguards that should be considered to ensure that these protections are effectively accomplished?*

The Coalition and ADI believe that the Government should direct federal agencies not to access or collect specific types of information that could violate privacy and civil liberties. For example, the Government should not access or collect personally identifiable information (PII), personal health information (PHI), or other sensitive financial or human resources information. If the Government does access or collect this information, it should not be used outside of the specific investigation and should be destroyed once the investigation is completed.

II. Discussion and Analysis – *d. Compliance When Operating in a Foreign Country*

Question 1: *Are there any specific situations you anticipate where your organization would be prevented from complying with the incident reporting or incident response requirements of FAR 52.239–ZZ due to country laws and regulations imposed by a foreign government? If so, provide specific examples that identify which requirements would be impacted and the reason that compliance would be prevented by the laws of a foreign government or operating environment within a foreign country.*

The Coalition and ADI are not currently aware of any specific situations of where our member organizations would be unable to comply with the proposed rule's incident reporting and response requirements. However, it is possible that our member organizations encounter such challenges during the rule's implementation period.

Question 2: *Do you anticipate situations where compliance with requirements in FAR 52.239–ZZ or alternative compliance methods (if added) would be prevented due to country laws and regulations imposed by a foreign government. If so, provide specific examples of when you expect such situations to occur, citing the authoritative source from the foreign government.*

As stated in our response to Question 2 of the previous section, the Coalition and ADI believe that the definition of "full access" in clause 52.239–ZZ(a) is sufficiently vague as to allow federal agencies to access <u>*any*</u> system belonging to a federal contractor. If this is the case, the U.S. Government would be able to demand access to servers that are physically located abroad. Here, federal agencies would be violating the sovereignty of foreign countries if they did not request authorization from local authorities before gaining access.

The Coalition and ADI also believe that 52.239–ZZ would allow federal agencies to access the personally identifiable information (PII) of consumers that have interacted with that federal contractor. If a federal contractor is located in the European Union, allowing the U.S. federal agencies to access and collect that PII could violate the General Data Protection Regulation (GDPR). Similarly, if that federal contractor regularly transfers data between the United States and the European Union, it may be in violation of its commitments under the EU-US Data Protection Framework Program. Therefore, the Coalition and ADI recommend that the Government specify that federal agencies will only be able to collect information from systems physical located within the United States. Furthermore, the Coalition and ADI recommend that the Government include language in the proposed rules stating that federal agencies are not allowed to access or collect PII, PHI, or other sensitive information that they encounter while accessing a federal contractor's systems.

II. Discussion and Analysis – *e. Security Incident Reporting Harmonization*

Question 1: *Timeline for reporting: Are there specific situations you anticipate where your organization will be required to report on different timelines in order to comply with the incident reporting requirements outlined in 52.239–ZZ, other Federal contract requirements, or other regulations promulgated under Federal law? How would your organization handle disparate cyber incident reporting timelines in other Federal Government contracting requirements or from other regulatory agencies?*

52.239–ZZ would require federal contractors to report a cybersecurity incident within "eight hours of discovery" and to "update the submission every 72 hours thereafter" until remediation activities are completed. To contextualize this requirement, the Coalition and ADI provide a list of federal cybersecurity incident reporting requirements below:

Table 1: U.S. Cybersecurity Incident Reporting Requirements

Regulation	Responsible Federal Entity	Timeline	Trigger	Covered Entities
FedRAMP Incident Communications Procedures[v]	GSA	1 hour	Discovery of Actual or Potential Incidents	Cloud Service Providers
HSAR 3052.204-72[vi]	DHS	1 hour for incidents involving PII / 8 hours for all others	Discovery of Actual or Potential Incidents	DHS Contractors
Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers[vii]	OCC; Federal Reserve; FDIC	36 hours	Determination of Actual Incidents	Financial Entities
DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting[viii]	DOD	72 hours	Discovery of Actual Incidents	Defense Contractors
Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)[ix]	CISA	72 hours	Discovery of Actual Incidents	Critical Infrastructure
Guidance on Public Company Cybersecurity Disclosures[x]	SEC	4 business days	Determination of Actual Incidents	Publicly Traded Companies

**Note: For the purposes of this table, 'discovery' means 'when company executives receive a call from their IT services that there *may be* an incident.' In contrast, 'determination' means 'when an incident response team confirms the incident through a forensic analysis.'*

Question 2: *Potential effect on incident response: 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 Coalition and ADI believe that the reporting requirements in 52.239–ZZ are overly burdensome and may limit a federal contractor's ability to respond to incidents. For example, 52.239–ZZ requires federal contractors to update their incident reporting every 72 hours regardless of if there has been any change in the status of the incident. This would require federal contractors to spend time updating reports without introducing new information. This requirement would reallocate resources that could otherwise be used for incident remediation. Similarly, both the 8-hour and 72-hour reporting requirements are disparate from other federal cybersecurity incident reporting requirements (as highlighted in our response to Question 1). This also increases the burden on federal contractors by increasing the complexity and costs of the compliance process. Accordingly, the Coalition and ADI firmly believe that the Government should seek to harmonize cybersecurity incident reporting requirements across its regulations, guidelines, and policies. However, if the Government sees sufficient reason to create a new timeline in this instance, we suggest that the Government at least revise 52.239–ZZ to require federal contractors to report a cybersecurity incident within "24 hours of the determination that an incident has occurred" and to "update the submission *when material changes occur*" until remediation activities are completed.

The Coalition and ADI would also highlight that federal contractors using third-party cybersecurity solutions receive multiple types of 'cybersecurity alerts' regarding their systems. In certain cases, network defenders may address an alert quickly enough that the event does not rise to the threshold of a cybersecurity "incident" (i.e., the adversary was not able to meaningfully achieve their objective). The Coalition and ADI recommend that the Government clarify that these types of events do not fall under the scope of "security incident" as defined in clause 52.239–ZZ(a).

Question 3: *Cost of providing ICT products and services: 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?*

Members of the Coalition and ADI believe that it is difficult to estimate the costs associated with providing ICT products and services to the Government before an incident occurs. Every cybersecurity incident is unique and requires different human, financial, and technical resources to address. Regardless, members of the Coalition and ADI agree that, if the Government creates shortened reporting timeframes, federal contractors will need to make infrastructure changes, hire more staff for their Cyber Security Incident Response Teams, and increase their compliance professionals to meet these additional requirements. Each of these efforts will pose a significant financial burden to federal contractors.

Question 4: *Scope of the contract clause: The proposed rule would require the new incident reporting clause to be included in all contracts involving ICT that are subject to the FAR, including those for commercially available off-the-shelf (COTS) items. This is broader in scope than, for instance, the DFARS clause. How would differences in scope between reporting requirements affect your organization's implementation of this clause?*

The Coalition and ADI believe that federal contractors may not always be able to meet the FAR incident reporting requirements for all contracts involving ICT. For example, in some cases federal contractors are third-party resellers, rather than the original software manufacturer. In these cases, the federal contractor can alert the Government about an incident affecting its own

systems, but not if there is an incident involving the software manufacturer. However, the proposed rules are not clear as to whether the Government could require software manufacturers to also abide by incident reporting requirements. Therefore, the Coalition and ADI urge the Government to clarify that these rules only apply the federal contractor, and that manufacturers cannot be held responsible for incident reporting that their intermediary agrees to in the contract.

The Coalition and ADI also believe that applying FAR's new incident reporting requirements to COTS products places an undue burden on companies. As a result of the rule, manufacturers would no longer be able to continue serving Government on commercial instances. For example, one of our members noted that the proposed rule's 8-hour notification timeline does not align with the existing global legal requirements that they already follow for their COTS products. Therefore, they would need to hire more staff and develop new U.S. Government-specific processes for their COTS products, creating a financial burden.

Question 5: *Definition of incident: The definition of ''security incident'' in the proposed rule incorporates the substantive provisions of the definition in 44 U.S.C. 3552, which has minor differences from with the definition of ''incident'' in Section 2209 of the Homeland Security Act of 2002 (as amended) and from the modified definition of ''covered incident'' used in CIRCIA, which is currently the subject of a separate rulemaking process, see 6 U.S.C. 681b(b). What, if any, additional implementation issues would your entity face complying with different definitions of an incident? How would your entity make the distinction between ''imminent jeopardy'' and ''actual jeopardy,'' and what effect could that have on the number of reported incidents that did not end up actually affecting confidentiality, integrity, and availability of information or an information systems?*

The Coalition and ADI believe the use of multiple definitions by the Government is adding an unnecessary burden to federal contractors. The Coalition and ADI recommend that the Government consistently use the definition of incident in 44 U.S.C 3552 across all reporting requirements.

According to our members, "imminent jeopardy" refers to a situation where there are clear and immediate indications that a security incident will occur *in the near future*. In contrast, "actual jeopardy" refers to a situation where a security incident is *currently happening* or has *already occurred*. In general, our members currently focus on reporting incidents under "actual jeopardy" because they are precise and non-disputable. Meanwhile, incidents under "imminent jeopardy" are less reported because there are too many variables to predict which incidents will occur with any degree of accuracy. Paying attention to incidents under imminent jeopardy requires substantial resources which could otherwise be used for remediation and recovery efforts. Moreover, incidents under 'imminent jeopardy' could be false positives. While members of the Coalition and ADI believe that there should be tools in place to monitor incidents under imminent jeopardy, the Government should not expect federal contractors to dedicate the same number of resources for both**.**

Moreover, the Coalition and ADI would highlight that the inclusion of COTS products in the FAR rule will pose significant complications to the incident reporting regime. Assuming manufacturers could handle the financial burden, the number of 'imminent' incident reports would still increase significantly. Federal agencies in receipt of these reports would then struggle to differentiate between important incidents and false positives.

[i] https://www.foia.gov/faq.html
[ii] https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf
[iii] https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf
[iv] https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident
[v] https://www.fedramp.gov/assets/resources/documents/CSP_Incident_Communications_Procedures.pdf
[vi] https://www.ecfr.gov/current/title-48/chapter-30/subchapter-H/part-3052/subpart-3052.2/section-3052.204-72
[vii] https://www.fdic.gov/news/board-matters/2021/2021-11-17-notational-fr.pdf
[viii] https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting.
[ix] https://www.congress.gov/117/plaws/publ103/PLAW-117publ103.pdf
[x] https://www.sec.gov/files/rules/final/2023/33-11216.pdf