May 20, 2024

John M. Tenaglia
Principal Director, Defense Pricing and Contracting
Office of the Secretary of Defense
Department of Defense
1400 Defense Pentagon
Washington, DC 20301

Karla Smith Jackson
Senior Procurement Executive, Deputy CAO, and Assistant Administrator for Procurement
Office of Procurement
National Aeronautics and Space Administration (NASA)
300 E St SW
Washington, DC 20024

Jeff Koses
Senior Procurement Executive
General Services Administration
1800 F Street, NW
Washington, DC 20405

Re: FAR Case 2021-017, "Federal Acquisition Regulation: Cyber Threat and Incident Reporting and Information Sharing"

Dear Mr. Tenaglia, Ms. Jackson, and Mr. Koses:

The Coalition for Government Procurement (the "Coalition") appreciates the opportunity to provide additional industry comments on FAR Case 2021-017.

By way of background, the Coalition is a non-profit association of firms selling commercial services, products, and solutions to the Federal Government. Our members collectively account for tens of billions of dollars of the sales generated through the GSA Multiple Award Schedules (MAS) program, VA Federal Supply Schedules (FSS), the Government-wide Acquisition Contracts (GWACs), and agency-specific multiple award contracts (MACs). Coalition members include small, medium, and large businesses that account for more than $145 billion in Federal Government contracts. The Coalition is proud to have worked with Government officials for more than 40 years towards the mutual goal of common-sense acquisition.

At the outset, the Coalition would like to point out that the stakeholder community has been focused on multiple cyber-related rulemakings under development, including DoD's Cybersecurity Maturity Model Certification (CMMC) Program 2.0, revisions to NIST 800-171, Software Bills of Materials, the implementation of the Federal Risk and Authorization Management Program (FedRAMP), cyber incident reporting generally, and the ongoing implementation of Section 889 (regarding the

restriction on the use of certain communications and video technologies). With so many initiatives underway, we believe that the Government and industry would benefit from opportunities for periodic information exchanges. Such exchanges would facilitate common understanding of the many compliance obligations involved in this space, and promote the efficient and effective implementation of cyber-related rules.

The Coalition supports the underlying objective of the cyber threat and incident reporting proposed rule to strengthen Federal cybersecurity and protect Government networks and we also urge the Council to consider the below questions and concerns raised by our members to promote vendor participation in the Government marketplace. Such participation increases competition and the benefits that flow therefrom and fosters agency access to the innovation needed to meet their missions.

Clarifying the Scope/Applicability of the Proposed Rule

The Coalition recommends clarifying the scope and impact of the new contract clause, FAR 52.239-ZZ, "Incident and Threat Reporting and Incident Response Requirements for Products or Services Containing Information and Communications Technology," and the new representation provision, FAR 52.239-AA, "Security Incident Reporting Representation." These provisions are set to be included in all solicitations and contracts, with no exceptions for contracts below the Simplified Acquisition Threshold (SAT) or for contracts for commercial products and services, or commercially available off-the-shelf (COTS) products. The proposed rule, however, provides that these provisions are meant to impact only contractors awarded contracts where information and communications technology (ICT) is used or provided in the performance of the contract, which is estimated to be 75 percent of all Federal contractors.

As written, the proposed rule does not explain what qualifies as "using" or "providing" ICT in the performance of a contract. Thus, the proposed rule should be clarified accordingly. Moreover, it should be recognized that including these provisions in all solicitations and contracts, even where they will not apply, will cause confusion for contractors and subcontractors as to whether compliance with the provisions is required under particular contracts.

The Coalition suggests the inclusion of an opt-out mechanism, similar to DFARS 252.239-7009, *Representation of Use of Cloud Computing*, which provides offerors the opportunity to check a box indicating whether they anticipate cloud computing services will be used in the performance of the contract or any subcontracts. Here, the relevant representation should indicate whether offerors anticipate ICT will be used in the performance of the contract or any subcontracts.

Further, members of the Coalition also ask the FAR Council to confirm that the reporting obligation in the new clause is to run prospectively from the date of inclusion of the clause in a contract.

Revising the Definition of a "Security Incident"

The proposed rule defines a Security Incident as the

> "***actual or potential occurrence*** of the following—
>
> (1) Any event or series of events, which pose(s) ***actual or imminent jeopardy***, without lawful authority, to the integrity, confidentiality, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies;
>
> (2) Any malicious computer software discovered on an information system; or
>
> (3) Transfer of ***classified*** or ***controlled unclassified information*** onto an information system not accredited (i.e., authorized) for the appropriate security level."
>
> Emphasis added.

With respect to reporting, the proposed rule requires contractors to submit a Cybersecurity and Infrastructure Security Agency (CISA) Incident Reporting Form for "all security incidents involving a product or service provided to the Government that includes information and communications technology, or the information system used in developing or providing the product or service" to CISA.

As currently written, our members feel this definition is overly broad. The reference to a "potential" occurrence should be removed to eliminate some of the ambiguity associated with the definition, which further defines a security incident to include events that pose "actual or imminent jeopardy." The Coalition also recommends that the definition be revised to tie it to confirmed incidents or impacts and/or have a materiality threshold for reporting. With respect to incidents involving information systems, we recommend that the definition be tied to systems dedicated to storing or processing government data rather than systems used in developing the product or service, which may include myriad systems and impose an undue burden on contractors. These recommendations narrow the definition and will help reduce over-reporting by contractors, thus preserving the utility of the CISA Incident Reporting System and facilitating CISA's identification of meaningful cyber incident reports.[1]

The FAR Council also should remove paragraph (3) of the definition in its entirety. Spillage of classified information is covered by separate regulations and is not contemplated for inclusion in this FAR Case per Executive Order 14028. Further, regulations relating to Controlled Unclassified

[1] The Coalition also asks that the FAR Council consider the implications of CISA's Cybersecurity Incident Reporting for Critical Infrastructure Act (CIRCIA) rulemaking in FAR Case 2021-017. Pursuant to the CIRCIA proposed rule, there is likely to be substantial overlap between the entities covered and the reporting obligations to CISA under both rules.

Information (CUI) are the focus of separate agency provisions and rulemaking. Inclusion here is likely to cause confusion among industry.

In addition, Coalition members suggest that the Government harmonize definitions of terms like "security incident" and "cyber incident" that already exist (*e.g.*, in the Defense Federal Acquisition Regulation Supplement (DFARS), Homeland Security Acquisition Regulation (HSAR), and for the FedRAMP) instead of creating a new definition that will necessarily lead to confusion and compliance burdens among industry.

Harmonizing Timing of Incident Reporting

The proposed clause requires submission of a CISA Incident Reporting Form within eight hours of discovery that a security incident *may have occurred* and a subsequent update every 72 hours thereafter. Such a short timeline is likely to inundate the government with false positive reporting, especially when combined with the overly broad definition of a "security incident." Moreover, our members have expressed that eight hours is not enough time to gather sufficient information for reporting and will take time away from industry personnel during such a key time needed to focus on mitigating the identified security incident.

Accordingly, the Coalition recommends that the Council harmonize the proposed rule with the 72-hour reporting requirement established by the DFARS and the CIRCIA to afford contractors more time to conduct initial investigations, prepare a preliminary report, and begin remediation efforts. Further, subsequent updates should be required only for material changes.

The Council should also consider exempting cloud service providers (CSPs) that have an existing FedRAMP authorization from the rule's reporting requirements so long as they comply with FedRAMP's incident communications procedures.

Revising the Definition of "Full Access"

Where the Contracting Officer, CISA, or the FBI request access to additional information or equipment in response to reported security incidents, the proposed rule requires contractors to provide "full access" to all contractor information systems used in performance, or which support performance, of the contract. Members of the Coalition request clarity regarding the scope of systems "used in performance" and "which support performance" of a contract. As currently drafted, systems that "support performance" of a contract could encompass all systems, which likely is not intended by the rule.

As currently drafted, this provision is overly broad and should be limited to align with similar provisions, such as DFARS 252.204-7012. Access should be limited to those systems dedicated to the government contract or those housing government data. Permitting this expansive level of access could put contractors in conflict with their contractual obligations and policies concerning confidentiality and privacy.

Software Bill of Materials (SBOM)

The Coalition recommends the SBOM requirements be removed entirely from the rule, as SBOMs seemingly are outside the proposed rule's intended scope. The proposed rule is intended to address cyber threat and incident reporting and information sharing, and standardized frameworks for SBOMs have not yet been developed. There still is some industry confusion surrounding the appropriate content and format for SBOMs. Thus, inclusion of this SBOM requirement in FAR Case 2021-017 likely will lead to inconsistent and unhelpful submissions to the government. Further, software supply chain security efforts are being addressed in a separate rulemaking (FAR Case No. 2023-002).

To the extent SBOM requirements are retained, members of the Coalition recommend that the collection of SBOMs be limited in scope, for example, only for critical software provided directly for use by the Government and not for all software used in performance of a contract. Alternatively, the Government should allow for the Secure Software Attestation Form, which was recently finalized, to be used to attest to compliance with secure software development practices rather than requiring SBOMs.

Subcontractors and Flow-Down Requirements

The proposed rule mandates that the new FAR clause be flowed down in all subcontracts where ICT is used or provided in the performance of the subcontract and requires subcontractors to notify the prime and the next higher tier subcontractor within eight hours of discovery of a security incident.

In addition to the aforementioned concerns regarding the definition of ICT and reporting requirements, prime contractors also are likely to face significant challenges obtaining compliance from subcontractors, namely from vendors of COTS products, who are likely to find these compliance obligations under the new FAR clauses to be untenable. COTS manufacturers may be unable to negotiate these clauses into upstream agreements and therefore would be unable to comply or represent compliance. Moreover, the additional cost of providing an SBOM to a reseller or to the Government may not necessarily be worth the cost to a COTS provider where the Federal market represents a negligible portion of its business. For these reasons, the Coalition requests the Council consider whether it can exclude or narrow the scope for COTS products suppliers, exclude commercial subcontractors from flow-down requirements, or consider whether a waiver process is possible to ensure access to products where compliance is not possible.

Based on the foregoing, we believe that both the Government and industry could benefit from meeting to discuss how the public and private sectors can work together to ensure that the many cybersecurity compliance obligations are executed efficiently and effectively, and to facilitate common understanding of the processes and the roles of the two parties in protecting our national security. The Coalition sincerely appreciates your consideration of such a meeting between the FAR Council, other critical Federal stakeholders and industry.

Thank you for your time and consideration.

Sincerely,

Roger Waldron
President

Cc: Christine Harada, Senior Advisor, Office of Federal Procurement Policy, Office of Management and Budget
Mathew C. Blum, Associate Administrator, Office of Federal Procurement Policy, Office of Management and Budget