THE COALITION
FOR GOVERNMENT PROCUREMENT

February 2, 2024

Ms. Carrie Moore
Procurement Analyst
General Services Administration
1800 F St NW
Washington, DC 20405

Re: FAR Case 2021–019 - Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems

Dear Ms. Moore:

The Coalition for Government Procurement ("the Coalition") appreciates the opportunity to submit these comments on the above-referenced proposed rule amending the Federal Acquisition Regulation (FAR) to provide standardized cybersecurity contractual requirements across Federal agencies for Federal information systems (FIS). The proposed rule seeks to do so by implementing recommendations received pursuant to the May 12, 2021 Executive Order 14028, ''Improving the Nation's Cybersecurity,'' and the Internet of Things (IoT) Cybersecurity Improvement Act of 2020 (Pub. L. No. 116–207).
By way of background, the Coalition is a non-profit association of firms selling commercial services, products, and solutions to the Federal Government. 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.

The Coalition supports the Federal Government's efforts to rationalize cybersecurity contractual requirements for FIS across Federal agencies. In this regard, the proposed rule lays out, in detail, material policies, procedures, and requirements for contractors to follow in the development, implementation, operation, and maintenance of FIS, both in iterations of the cloud and in the non-cloud context, and it included provisions related to the acquisition of services for the foregoing.

These services are complex, and their acquisition and implementation will involve significant compliance obligations and activities. For this reason, the Coalition emphasizes the need for the Government to state unambiguously in its solicitations and contracting documents whether the contractor will be maintaining a FIS and whether the new requirements apply. Contractors should not be placed in the position of guessing whether FIS are involved in their contracts and their associated compliance status. Further, the Government could consider including an opt in/out representation in solicitations similar to that in DFARS 252.239-7009 for cloud computing to allow for a clearer designation of whether the requirements will be expected to apply.

In addition, the Coalition submits the following member comments/recommendations:

I. Government Access to Contractor Information.

Proposed clause 52.239-XX requires contractors to grant the government full access, physical and electronic access, to information systems used in performance, or which support performance of the contract. Granting full access to the government could require contractors to breach other obligations. The final rule should incorporate the suggested definition of full access below so that contractors can meet the government's requirements while also maintaining the integrity of their business relationships, contracts, and agreements.

Full access means, for all contractor information systems used in performance, ~~**or which support performance,**~~ of the contract—

(1) ~~**Physical and**~~ Electronic access to—

(i) Contractor networks that are dedicated to government data,

(ii) Systems that are dedicated to government data,

(iii) Accounts dedicated to Government systems only,

~~**Other infrastructure housed on the same computer network,**~~

(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, and

(iii) Event information, ~~and~~

~~**(iv) Statements, written or audio, of contractor employees describing what they witnessed or experienced in connection with the contractor's performance of the contract.**~~

II. Definition of government-related data. The definition of government-related data excludes important exceptions to government-related data. The changes below are recommended.

"*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, that do not incorporate Government data. ~~**that are not primarily applied to the Government data.**~~

III. Cloud Computing Security Requirements. Subparagraph (c) of the proposed clause 52.239-XX conflates the responsibilities of contractors using cloud computing to provide their own information technology services in support of a government contract with the services that a

cloud service provider provides as a prime government contractor. To avoid this ambiguity, this final rule should use the language used DFARS 252.204-7012(b)(2)(ii)(D), copied below for reference.

"*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 (https://www.fedramp.gov/resources/documents/) 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*."

IV. Program of Inspection.
Section (f)(3)(i) of proposed clause 52.239-XX is redundant because the continuous monitoring requirements of the FedRAMP program meet this requirement, along with government's audit, investigation, and inspection rights as specified in the rest of the proposed clause.

V. Indemnification of the government. The indemnification portion of the proposed clause is extremely broad and appears to be unreasonable given that it would apply to commercial contracts. The indemnification obligation already established in FAR clause 52.212-4(h) is sufficient in protecting the government and fair and reasonable for the contractor to comply. The final rule should remove the indemnification portion of the proposed clause 52.239-XX and rely on the already established FAR clause 52.212-4(h).

Thank you again for the opportunity to submit these comments on FAR Case 2021–019 - Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems. If you have any questions, please contact me at rwaldron@thecgp.org or (202) 331-0975.

Best regards,

Roger Waldron
President