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 2021-019

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 2021-019. We hope that our comments will lead to further clarification and revision of the FAR rules so that industry may effectively adapt to new standardized cybersecurity contractual requirements for Federal Information Systems (FIS).

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 federal 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.

We would like to highlight several recommendations related to the following subject areas:

1. **Access to contractor systems**

   In the proposed rule, clause 52.239–XX and clause 52.239–YY both require federal contractors to provide the Government (i.e., CISA, the FBI, or another civilian agency) with "full access" to "all contractor information systems used in performance, or which supports performance, of the contract." This includes "physical and electronic access to (i) contractor networks, (ii) systems, (iii) Accounts dedicated to Government systems, (iv) other infrastructure housed on the same computer

network, (v) Other infrastructure with a shared identity boundary or interconnection to the Government system." It also includes the "provision of all requested Government data or Government-related data, including (i) images, (ii) log files, (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."

This language would provide the Government with unbounded access to all a federal contractor's systems, including information belonging to the federal contractor, its employees, and its non-federal clients. As highlighted in our response to FAR Case 2021-017, the Coalition and ADI believe that expecting a federal contractor to allow this degree of access to its systems simply because it is selling to the Government is both unreasonable and unprecedented. Clause 52.239–XX(f)(3) and clause 52.239–YY(f)(3) in FAR Case 2021-019 are even more egregious than FAR Case 2021-017 because they provide the Government with full access so that it may "carry out a program of inspection to safeguard against threats and hazards to the security … and privacy of Government data." Here, the Government is not only unbounded in terms of which systems it can access, but also in terms of when it can access them since "threats and hazards" are not defined.

To address this problem, the Coalition and ADI urge the Government to eliminate the "full access" provision by removing clause 52.239–XX(f)(3) and clause 52.239–YY(f)(3) from 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 federal contractors to provide it with 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.[1]

- 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. This would prevent the Government from accessing systems belonging to the federal contractor's non-federal clients. To accomplish this, the Government could redefine "full access" in clause 52.239–XX(f)(3) and clause 52.239–YY(f)(3) so that it has the following meaning:

[1] https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

- "*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).

2. **Use of Government-related data**

In the proposed rule, the Government defines "Government-related data" as "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." Federal contractors are not allowed to "access, use, or disclose Government data or Government-related data unless specifically authorized under the contract or task or delivery order or in writing by the Contracting Officer." In these cases, the federal contractor may only use Government-related data "to manage the operational environment that supports the Government data and for no other purposes unless otherwise permitted with the prior written approval of the Contracting Officer."

The Coalition and ADI believe that restricting the use of Government and Government-related data would undermine the opportunity to enhance the security and functionality of commercial products and services provided to the Government. Cloud service providers (CSPs) regularly use data generated from customers' interactions with their services to analyze and improve their underlying technology. For example, federal contractors use threat indicators and malicious files discovered in user data – including Government or Government-related data – as packet transfer information to generate future threat signatures. This benefits the federal contractor providing the cloud service, the federal agency procuring the service, and all the federal contractor's other federal and non-federal customers.

Therefore, the Coalition and ADI recommend that the Government narrow the scope of the definition of "Government-related Data". We urge the Government to redefine "Government-related data" in clause 52.239-XX(a) and clause 52.239-YY(a) to have 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."

3. Cloud computing security requirements

In the proposed rule, clause 52.239-XX(c) requires federal contractors to "implement and maintain security and privacy safeguards and controls with the security level and services required in accordance with the Federal Risk and Authorization Management Program (FedRAMP) authorization level specified." It also requires federal contractors to "engage in continuous monitoring activities and provide continuous monitoring deliverables" as required by FedRAMP.

The Coalition and ADI believe that this language is unclear and may conflate the responsibilities of federal contractors providing cloud computing services to the Government, federal contractors using third-party cloud computing services for the performance of a federal contract, and federal contractors using cloud companies using third-party cloud computing services for their own internal purposes. To avoid this ambiguity, this final rule should also include the language used DFARS 252.204-7012(b)(2)(ii)(D):

"*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*."

4. Indemnification Clauses

In the proposed rule, clause 52.239-XX(h) and clause 52.239-YY(m) ("the indemnification clauses") oblige a federal contractor to "indemnify the Government and its officers, agents, and employees acting for the Government" against certain liabilities arising out of the performance of the contract. Specifically, this includes costs and expenses incurred because of the federal contractor's introduction of certain information into Government data or the federal contractor's unauthorized disclosure of certain information.

This provision is a significant departure from how risks are currently handled in Government contracts. The change to a stricter liability would hold federal contractors at fault regardless of the facts surrounding an incident or disclosure. Additionally, the removal of the federal contractor defense provision would hold a federal contractor liable even if they are operating within the terms of the contract.

This shift of risk would also increase costs for both federal contractors and the Government. For example, increased liability will either make it more difficult for federal contractors to get insurance or raise their premiums on their existing policies. This would particularly affect small and medium-size federal contractors, which would not be able to afford proper coverage. In turn, the Government would incur higher costs as the number of federal contractors in the marketplaces decreases.

The Coalition and ADI would also highlight that the Government already has ample methods and mechanisms to enforce contractual provisions. For example, the False Claims Act enables the Government to seek three times the damages incurred for a material breach of contract. Furthermore, the FAR itself already has an indemnification obligation at clause 52.212-4(h). This provision alone is sufficient to protect the Government and would be fair and reasonable for federal contractor compliance. Therefore, to avoid chilling federal contractor participation in the marketplace, the Coalition and ADI believe that the government should remove clause 52.239-XX(h) and clause 52.239-YY(m) from the proposed rule.

5. Data Localization

In the proposed rule, clause 52.239-XX(c) states that "for cloud computing services required to meet FIPS Publication 199 high impact requirements, the Contractor shall maintain within the United States and its outlying areas (see FAR 2.101) all Government data that is not physically located on U.S. Government premises, unless otherwise specified in the contract." This provision conflicts with the Office of Management and Budget's (OMB) draft FedRAMP Guidance, which says "FedRAMP should not incentivize or require commercial cloud providers to create separate, dedicated infrastructure for Federal use, whether through its application of Federal security frameworks or other program operations."[2] While certain classifications of data may still necessitate specialized government controls (i.e., International Traffic in Arms Regulations (ITAR) data and certain types of Controlled Unclassified Information (CUI)), this should not be the default model for all FIS.

Therefore, the Coalition and ADI urge the Government to eliminate clause 52.239-XX(c) and remove any references to data localization from the proposed rule. If this is not possible, the Government should at least specify that data localization does not include security data (e.g., Network telemetry data, URLs, metadata, net flow data, origin and nature of malware, and other TTPs; Threat intelligence from the public-facing internet; Vulnerability data: Common Vulnerability Enumeration (CVE) and other structured, or unstructured, context about vulnerabilities; Indicators of Compromise (IOCs) and other signature-based identifiers of cyber risk, etc.)

[2] https://www.cio.gov/assets/files/resources/FedRAMP-updated-draft-guidance-2023.pdf