February 2, 2024

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

Comments from the CSP-AB regarding FAR Cases 2021-017: Cyber Threat and Incident Reporting and Information Sharing; and 2021-019: Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems

Dear Mr Clark,

The Cloud Service Providers-Advisory Board (CSP-AB) welcomes the Administration's implementation of Executive Order 14028 Improving the Nation's Cybersecurity ("the E.O.") through the federal acquisition regulations. In effectuating Section 2 of the EO, Federal Acquisition Regulation (FAR) Cases 2021-017 and 2021-019 implement new, burdensome regulatory guidance on information technology companies who are already meeting a high security and compliance bar across the federal marketplace.

The CSP-AB represents the world's leading cloud companies and supports standards and policies that promote and enable secure cloud adoption in the public and private sectors. Our member companies are global leaders in the drive to provide safe, scalable, and accredited digital government services, with a focus on both the civil servants delivering those services and the end-users receiving them.

Collectively, our members hold over 700 Authorities to Operate (ATOs) across all service models and impact levels. FedRAMP provides a scalable mechanism to accelerate agency cloud adoption by creating processes for security authorizations and allowing agencies to leverage security authorizations at scale. The members of the CSP-AB have an ongoing relationship with the US Government and third-party assessment organizations (3PAOs) since the inception of FedRAMP in 2011. The CSP-AB champions the continued leverage of FedRAMP to meet the government's needs. Our members are already subject to the many regulatory requirements envisioned by the Federal Acquisition Regulatory Council (FAR Council).

We recommend that the FAR Council leverage FedRAMP accreditation for software providence disclosures and generally focus on implementing the Administration's goal of regulatory harmonization when considering whether to levy net-new burdens on the government contractor community. FAR proposed rule 2021-019 *Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems* fully leverages FedRAMP for cloud services providers; however, we see a missed opportunity to leverage FedRAMP in proposed rule

2021-017 *Cyber Threat and Incident Reporting and Information Sharing*. FedRAMP has incident reporting protocols and a mechanism that would meet the requirements of proposed rule 2021-017 for cloud service providers. Additionally, FedRAMP could be leveraged for CSPs to meet the proposed SBOM requirements. To further promote harmonization across the government, this final rule for 2021-017 should require the use of the existing FedRAMP protocols and procedures for incident reporting and SBOM collection, as detailed herein, for CSPs.

I. Application of the Rules to CSPs

A. Shared Responsibility Model. Many third-party technology providers, such as infrastructure cloud service providers (CSPs), often serve as both contractors to the government and also provide services to government contractors. CSPs work with customers to employ the shared responsibility model for cybersecurity risk management. In this model, a CSP is responsible for protecting the infrastructure that runs all of the services offered in the cloud, which includes the hardware, software, networking, and facilities delivered by the CSP. The organization (i.e. the CSP's customer) is responsible for choosing the appropriate services, and properly configuring and managing them to achieve the needed security outcomes. The organization's responsibility will vary based on the services they choose, the integration of those services into their IT environment, and applicable laws and regulations. Security incidents can occur on either side the of the shared responsibility model. CSPs can support their customers to prevent and detect security incidents on their side of the shared responsibility model; however, reporting requirements should ensure that CSPs and their customers are only responsible for reporting incidents and managing data that occur on their respective sides of the shared responsibility model. For example, the data preservation requirements detailed in clause 52.239-ZZ (c)(1)(i) of proposed rule 2021-017 *Cyber Threat and Incident Reporting and Information Sharing,* copied below for reference, could require a contractor to infringe upon their customers' rights and responsibility in accordance with the shared responsibility model. The final rule should include language that allows contractors to maintain their customer relationships without breach.

"(c) *Supporting incident response.*
(1) *Data preservation and protection.*

> (i) The Contractor shall collect, and preserve for at least 12 months in active storage followed by 6 months in active or cold storage, available data and information relevant to security incident prevention, detection, response and investigation within information systems used in developing or providing ICT products or services to the Government. This data includes, but is not limited to, network traffic data, full network flow, full packet capture, perimeter defense logs (firewall, intrusion detection systems, intrusion prevention systems), telemetry, and system logs including, but not limited to, system

event logs, authentication logs, and audit logs. Upon request by the Contracting Officer, the Contractor shall promptly provide this data and information to the Government. (ii) When the Contractor has discovered that a security incident has occurred on an affected information system, the Contractor shall immediately preserve and protect images of all known affected information systems that impact the federal government's systems and all available monitoring/packet capture data…"

As the federal government endeavors to promote harmonization of cyber incident reporting across regulations, guidelines and polices, please consider the aforementioned and determination that FedRAMP in consultation with OMB made regarding M-21-31. The determination was made that the requirements of M-21-31 do not apply directly to Cloud Service Provider (CSP) offerings unless that CSP is a government system; this determination is applicable to this FAR case and the associated requirements and resulting clauses. This final rule should reflect this determination by noting that CSPs are required to support agency requirements to comply with FAR clause 52.239–ZZ Incident and Threat Reporting and Incident Response Requirements for Products or Services Containing Information and Communications Technology; however, they are not principally responsible for meeting the requirements themselves unless that CSP is a government system. CSPs are encouraged to align with FAR clause 52.239–ZZ where possible.

B. Cloud Computing Security Requirements. Proposed rule 2021-019 *Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems,* 52.239-XX(c) 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*."

C. Program of Inspection. Proposed rule 2021-019 *Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems* clause 52.239-XX Section (f)(3)(i) is redundant because the continuous monitoring requirements of the FedRAMP

program meets this requirement along with government's audit, investigation and inspection rights as specified in the rest of the proposed clause.

II. SBOM Requirements

A. SBOM Collection for CSPs. SBOMs should not be collected for cloud service offerings, as they are subject to frequent change, and the Cloud Service Provider (CSP), rather than the end user, is responsible for applying required security updates, based on information contained in the SBOM.

Rather, to accomplish the government's goal of encouraging the private sector to "adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace" the government should allow CSPs to demonstrate their maintenance of software provenance through the FedRAMP program, with verification from a 3PAO. One option would be to allow CSPs to select NIST SP800-53 Rev. 5, SR-4 Provenance control into their baselines.

SBOMs, particularly for cloud service offerings, provided to the government present a risk, especially if centrally stored without guaranteed technical safeguards. If exposed, SBOMs give malicious actors significant information to help target their vulnerability discovery work. Disclosure of this information creates new risks that are not currently present in the cloud services ecosystem.

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.

If the Government does move forward with collecting SBOMs from all contractors, the Government must provide proper access controls, encryption at rest, and assume liability in the event of disclosure to non-authorized actors causes harm to the provider of the SBOM.

There are three high level categories of how software is consumed, direct, indirect and as-a-service, see description below. In the case of direct consumption and indirect consumption the software consumer has agency in applying vendor updates. In the case of software consumed as a service the software consumer does not have agency in applying updates, it is wholly on the part of the software provider.

i. Direct consumption (e.g., download from internet, installation from install media).
ii. Indirect consumption (e.g., use of a hosted MySQL solution in which the hosting provider asks the user to schedule 'maintenance windows' in which to accept a patch).
iii. As-a-service consumption (e.g., 'cloud software' where the user only interacts with the software through a set of APIs).

Given the risks associated with collecting and safeguarding SBOMs from various USG contractors, we recommend that the government start with a pilot program to collect SBOMs only for packaged software, while allowing cloud offerings to demonstrate software provenance through the recommendations mentioned above. The government could evaluate the security benefit of the collection of SBOMs for packaged software, along with the efficacy of allowing CSPs to demonstrate their software provenance tracking through the FedRAMP Program, before imposing SBOM collection requirements on cloud service offerings.

When monitoring SBOMs (or software provenance data) for embedded software vulnerabilities as they are discovered, Cloud Service Providers should provide the government with assurance, through a 3PAO, they have in place:

i. A software provenance tracking system
ii. A vulnerability management process
iii. An incident response plan.

The Government's role would be to regularly verify that these systems and processes are in place through the FedRAMP Program.
For cloud service offerings, the code is updated many times to day (up to hundreds of times), so there will be challenges in the volume of SBOMs produced and there is no efficient way to provide the government with daily updates of the SBOMs. This is why it is better to leverage the FedRAMP Program, which CSPs must adhere to in order to provide cloud services to the U.S. government, to verify that a CSP maintains software provenance rather than collecting SBOMs.

Also, once alerted to a risk, based on the contents of an SBOM the consumer of the software must have an agency update that software and/or apply configuration changes to mitigate the identified risk. This is the key element of SBOMs, they provide value only when the consumer of that software has agency in mitigating risks identified by elements found within an SBOM.

Sincerely,

Laura Navaratnam

Executive Director

The Cloud Service Providers - Advisory Board

https://www.csp-ab.com/