February 2, 2024

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

Dear Mr. Clark:

BSA | The Software Alliance[1] appreciates the opportunity to respond to the proposed Federal Acquisition Regulation: Cyber Threat and Incident Reporting and Information Sharing (FAR Case 2021-017). BSA has a long history of supporting efforts to improve cybersecurity and believes that partnership between federal and international governments and industry is the most direct path toward a more secure future.

BSA is the leading advocate for the enterprise technology sector. Our members are among the world's most innovative companies and help to drive digital transformation by providing the solutions that make businesses and government agencies more competitive and effective, including cybersecurity; identity, credentialing, and access management; human resources management; customer relationship management; design and modeling; collaboration and communication; data analytics, visualization, and backup; and ticketing and workflow solutions.

First, BSA is concerned about the lack of harmonization of the proposed rule and the numerous other US Government, international, and private sector efforts to improve the cybersecurity of US Government agencies. The issue of harmonization is of the utmost importance, which is why BSA included harmonizing government laws and policies as a top

[1] *BSA's members include: Adobe, Alteryx, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, Databricks, DocuSign, Dropbox, Elastic, Graphisoft, Hubspot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Okta, Oracle, PagerDuty, Palo Alto Networks, Prokon, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Workday, Zendesk, and Zoom Video Communications, Inc.*

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

priority in both BSA's Procurement Agenda and BSA's 2024 Global Cyber Agenda. Our concern about harmonization is not limited to the rules proposed incident reporting requirements, though those proposed requirements do create serious concerns, discussed in detail below. Generally, when harmonization is based on best practices and internationally recognized standards it supports efficiency, resilience, and security.

BSA recommends that the FAR Council, in collaboration with the OFCIO at OMB, work towards harmonizing the range of draft regulations and guidance that are currently out for industry comment and review. These include the OMB's recently closed memo on Artificial Intelligence and the draft FedRAMP memo as well as the Department of Defense's (DOD) Cybersecurity Maturity Model Certification (CMMC) 2.0, and the Cybersecurity and Infrastructure Security Agency's (CISA) proposed regulations implementing the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA). There are significant changes to the larger federal IT environment that could potentially conflict and require significant changes to the enterprise software that is sold to the US Government. We understand that the Council is contemplating two additional rules: FAR-2021-0019 Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems and FAR-2023-06 Implementation of Federal Acquisition Supply Chain Security Act (FASCASA) Orders. We applaud the FAR Council for looking at these three FAR rules in concert, but also urge that they look at the other memos and regulations that will have impact on the purchasing environment for software.

We urge the FAR Council to consult with stakeholders across government and industry to look at these changes in concert, as the multiple regulations will need a coordinated approach to advance AI innovation through modernized IT.

In addition to these general concerns, BSA offers the following specific responses to the questions the FAR Council posed.

## I. Do Not Mandate Law Enforcement Access to a Contractor's Information Systems and Its Customer's Information

The proposed rule includes changes to paragraph (c)(6) of the clause at FAR 52.239-zz that would provide CISA, the Federal Bureau of Investigation (FBI), and the contracting agency "full access" to applicable contractor information and information systems.

As noted elsewhere in the proposed rule, "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." This proposed rule seems to forget or ignore what both EO 14028 and the Constitution recognize. Instead, the proposed rule would give law enforcement a staggering amount of access to the information and information systems of private companies, without clear protections for the private and sensitive personal data often stored in such systems and without any safeguards against the intentional or negligent misuse of such unrestricted

access. We strongly recommend deleting this requirement from the proposed rule, for at least two reasons.

First, the proposed rule undermines privacy and security protections. Under the proposed rule, a contractor would be required to provide "full access and cooperation" to CISA, the FBI, and the contracting agency, if any of those entities determine such access is needed to investigate or respond to an incident. The proposed rule only includes one limit on such sweeping access: requiring the contractor to confirm a request from CISA or the FBI is authentic by contacting the agency prior to granting access. The proposed rule fails to offer any substantive protections for information held on the contractor's systems, or any limits on the length and extent of the government's access. This requirement may provide access to not just the contractor's own data (which may be commercially sensitive or involve trade secrets) but also the personal data of individuals stored on that contractor's system. For example, a contractor may provide both government-facing services to the contracting agency and consumer-facing services directly to individuals. As a result, providing access to a contractor's system could inadvertently grant CISA or the FBI access to information about individual consumers who have no relation to the government-facing service that was breached.

Second, the proposed rule broadly undercuts the United States Government's goal of procuring secure and reliable technologies that keep information private. Contractors should be encouraged to adopt privacy-protective and security-protective practices, including limiting access to both their overall services and to the data stored on those services. Requiring contractors to allow "full access" to their systems undermines these goals, and will result in less private and less secure services. In addition, this type of access will create challenges for contractors operating in foreign countries, particularly when the contractor also serves foreign customers that require the contractor to commit to strict limits on how governments can access information stored with the contractor.

For example, Section zz(c)(1) would require a contractor to "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 . . . this data includes network traffic data, full network flow, full packet capture, perimeter defense logs." This requirement undermines privacy and is overly burdensome. The burdens of the requirement might be addressed by simply requiring retention, (i.e. eliminating the distinction between active and cold storage), and reconsidering what other data is truly necessary and reasonable for a contractor to collect and preserve, for example, full network flow and full packet capture.

Finally, the proposed rule also requests information about the international impacts of mandating US Government access to contractor information. Many foreign governments – including like-minded allies – are concerned with US Government agencies obtaining access to information. Governments have proposed or enacted laws and policies that would limit market access to companies that are required to provide such access or

otherwise lack sufficient privacy protections, for example the European Union's Cybersecurity Certification Scheme (EUCS) or France's SecNumCloud. In short, mandating law enforcement access to a contractor's information systems and its customer's information would create significant challenges for any company that operates outside the US.

We strongly recommend the proposed rule be revised to eliminate this requirement.

## II. Do Not Require Contractors to Develop or Maintain a Software Bill of Materials

The proposed rule would require contractors to develop and maintain a software bill of materials (SBOM).

BSA supports the development and use of SBOMs. We believe that current collaboration between governments and industry will result software producers having a clear understanding of what information to include in an SBOM and in what format as well as customers being prepared to leverage that information. We particularly appreciate the FAR Council's understanding that SBOMs are useful for incident response but not a panacea for all cybersecurity challenges.

Secure software development is the top priority in BSA's 2024 Global Cyber Agenda, but today, that priority is more effectively achieved through the use of secure software development best practices like those found in BSA's Framework for Secure Software or the National Institute of Standards and Technology's Secure Software Development Framework (SSDF), or through other mechanisms such as CISA's development of a Secure Software Development Attestation Common Form.

The FAR Council should not require contractors to develop and maintain SBOMs at this time for two related reasons. First, SBOMs are not ready. Governments and industry are working to develop and standardize SBOMs so that software producers can create them but also so that customers can use them. Much of this work is being led by the CISA, and includes weekly meetings of government and industry experts to work on the vulnerability exploitability eXchange (VEX) model, sharing and exchanging SBOMs, adoption of SBOMs, and tooling and implementation of SBOMs. Supporting these continued efforts, rather than adding requirements before stakeholders have finished their work, will advance the FAR Council's goals.

Second, requiring contractors to develop and maintain an SBOM would undermine harmonization of SBOM requirements as US Government agencies are currently working to develop a holistic approach to SBOMs. Again, the cybersecurity community is hard at work to develop and standardize SBOMs, and other US Government efforts, for example CISA in the Secure Software Attestation Form, have explicitly declined to require software producers to develop and maintain an SBOM.

If the FAR Council aligns its work with the US National Cybersecurity Strategy, it must work toward harmonization with the broad swath of proposed laws and policies that are currently being contemplated or implemented.

BSA suggests the FAR Council revisit requirements relating to SBOMs after the cybersecurity community completes its on-going efforts and ensures its requirements are harmonized with these efforts.

## III. Harmonize Security Incident Reporting with Existing Law

The proposed rule includes changes that require a contractor to

> *immediately and thoroughly investigate all indicators that a security incident may have occurred and submit information using the CISA incident reporting portal . . . within eight hours of discovery . . . [and to] update the submission every 72 hours thereafter until the Contractor, the agency, and/or any investigating agencies have completed all eradication or remediation activities.*

As the proposed rule notes

> *When the same underlying systems are subject to inconsistent or contradictory incident reporting requirements--or where such requirements are duplicative but enforced differently by different counterparties or regulators--companies may focus more on compliance than on security, which can result in passing higher costs on to customers, including the Government.*

The National Cybersecurity Strategy states plainly, the US's "strategic environment requires . . . regulatory frameworks that are harmonized to reduce duplication." Here, the proposed rule's heading "e. Security Incident Reporting Harmonization" suggests the FAR Council seeks to harmonize its requirements. And yet, the proposed rule fails to harmonize its requirements with those set forth in CIRCIA.

At the absolute minimum, the FAR Council should align the types of incidents a contractor would be required to report as well as the timing of those reports. For example, the proposed rules use of the phrase "may have occurred," suggesting that the FAR Council intends contractors to submit information to CISA regarding potential incidents. In contrast, CIRCIA requires a covered entity to report when it reasonably believes it has become the victim of a covered cyber incident. The proposed rule would trigger an inordinate amount of activity in response to potential incidents that ultimately are determined not to be incidents – an outcome Congress explicitly attempted to avoid. Put plainly, the effect of this requirement would move resources better invested in responding to actual incidents to providing information to the US Government regarding false positives.

Unfortunately, the proposed rule ignores existing cyber incident reporting requirements like those found the Critical Infrastructure Cyber Incident Reporting Act (CIRCIA) and creates yet another scheme for reporting cyber incidents. BSA suggests the FAR Council harmonize its reporting requirements with those being promulgated pursuant to CIRCIA.

## IV. Reconsider Its Scoping of "Government-Related Data"

The proposed rule defines "government-related data" as any information, document, media, or machine-readable material regardless of physical gorm or characteristics that is created or obtained by a contractor through the storage, processing, or communication of Government data" but explicitly excludes "(1) A contractor's business records (e.g. financial records, legal records) that do not incorporate Government data, or (2) Data such as operating procedures, software coding or algorithms that are not uniquely applies to the Government data."

Such a narrow scope would encumber the standard practice of using a customer's data to improve the security of products and services. Contractors regularly use customer data to analyze and improve their products and services. For example, a contractor will use threat information from one user's data to enhance its products or services both for that customer and for all its other customers. This use benefits both the specific customer, the contractor's other customers, and the entire digital ecosystem.

BSA suggests that the FAR Council exclude standard commercial practices, for example, using data to enhance a product or service from the definition of government-related data.

## V. Reconsider Including Requirements Related to IPv6

The proposed rule would require contractors to complete activities related to the implementation of IPv6. As the proposed rule states, it is focused on revising the FAR pursuant to Executive Order 14028 on Improving the Nation's Cybersecurity (EO 14028). Importantly, EO 14028 does not contemplate the transition to IPv6.

The journey to IPv6 has been in the works since the late 20th Century and the transition is an important step for the entire digital ecosystem. The US Government's own transition has included numerous types of documents from research papers to implementation memoranda. In 2020, OMB issued M-21-07 on Completing the Transition to Internet Protocol Version 6. BSA supports efforts by the OMB OFCIO and the CIO Council to complete this transition. However, because EO 14028 does not contemplate the transition to IPv6, BSA suggests the FAR Council remove requirements related to IPv6 from the final rule.

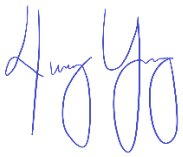
## VI. Clarify the Rule Applies Only Prospectively

Even if the FAR Council improves the proposed rule to address the challenges identified above, the FAR Council should also clarify that the rule applies only prospectively, that is to new contracts or future cyber incidents. Prospective application will provide fairness and

legal certainty while reducing unintended consequences and easing administrative burden. Most importantly, the FAR Council can achieve its goal of increasing the protection of US Government networks without creating resource intensive retroactive reporting requirements.

*  *  *

BSA Appreciates the opportunity to provide the above information and looks forward to working with the General Services Administration to advance its mission and improve the cybersecurity of the entire digital ecosystem.



Henry Young

Senior Director, Policy