2101 Wilson Boulevard, Suite 700, Arlington, VA 22201-3060 • (703) 522-1820 • (703) 522-1885 Fax • NDIA.org

February 2, 2024

Ms. Marissa Ryba
Procurement Analyst
General Services Administration

Electronic Submission: www.regulations.gov, FAR Case 2020-017

Re: Request for Comment on FAR Case 2020-017, Cyber Threat and Incident Reporting and Information Sharing

Dear Ms. Ryba:

The National Defense Industrial Association (NDIA) appreciates the opportunity to provide feedback on the proposed rule for FAR Case 2021-017 to partially implement Executive Order (E.O.) 14028 on cyber threats, incident reporting, and information sharing and OMB Memorandum M-21-07, *Completing the Transition to Internet Protocol Version 6 (IPv6)*.

NDIA is the nation's oldest and largest defense industry association, representing nearly 1,750 corporate and over 65,500 individual members from small, medium, and large contractors, a majority of which are small businesses. Our members engage daily with the federal government's mission areas, including national and homeland security apparatuses. They are well-versed in the array of cybersecurity requirements and standards across the Federal Government and in addressing and mitigating cyber incidents in information systems.

NDIA fully supports the overarching policy objectives behind E.O. 14028, including that the "prevention, detection, assessment, and remediation of cyber incidents is a top priority and essential to national and economic security." At the same time, NDIA is committed to creating a unified cybersecurity standard for government acquisitions. To that end, as set forth more specifically below, NDIA submits the Proposed Rule does not meet that objective and would cause more challenges and drive more costs into the government mission.

The Proposed Rule conflicts with existing regulations and reporting requirements of the Department of Defense (DoD), National Industrial Security Policy Operating Manual (NISPOM), Securities and Exchange Commission (SEC), Department of Homeland Security (DHS), and European Union (EU). The Proposed Rule also imposes significant requirements and risks for contractors of all sizes across the government supply chain, creates gaps in requirements, and leaves some key questions unanswered. In this regard, the proposal vastly underestimates the impact of the cyber incident reporting and Software Bill of Materials (SBOM) requirements regarding time, cost, and personpower. Lastly, the Proposed Rule includes the requirement for implementation of IPv6, which does not concern cyber incident reporting and would require a transition of hardware across varying levels of capability of contractors in the supply chain. To create a more unified cyber standard for government contracting, NDIA offers the following comments and suggestions:

1. The Proposed Rule Lacks Consistency and Creates an Undue Burden of Reporting Requirements.

   COMMENT: As recognized in the Federal Register, the 8-hour reporting requirement in the Proposed Rule is inconsistent with other reporting requirements within different agencies. For example, it is much shorter than the 72-hour reporting requirement under DFARS 252.204-7012 and the Cyber Incident

Reporting for Critical Infrastructure Act, which expresses Congressional intent on this subject. It also differs from the reporting requirement in the NISPOM, which the rulemaking itself reflects "prompt" reporting. The need for such a short reporting window provides little actionable value to the government and, at the same time, undercuts the ability of a contractor to focus its resources on addressing the immediate cyber incident's impacts so it can continue to perform its government contracts and engage in remediation. Mandating an 8-hour reporting requirement, without any safe harbor, will divert the focus of contractors from the performance of essential tasks to ensure their protection of systems and viability to perform. Further, requiring ongoing and repetitive reporting every 72 hours thereafter will also divert resources from follow-up activities needed for remediation. These actions increase the costs and raise the risk of liability for contractors.

RECOMMENDATION: Harmonize the reporting requirement with other federal efforts to report cyber incidents to maintain a consistent expectation among contractors about when reporting must be made. It is more important to understand the government's ability to make the reported information actionable. Additionally, the FAR Council should insert a safe harbor provision so that contractors do not face the risk that any initial and interim reporting, which may not be complete, will not place them in a position where they face potential false claims risks and liabilities. A safe harbor provision will also incentivize contractors to be more forthcoming in their reporting.

2. The SBOM Requirement is Overly Broad.

COMMENT: The proposed SBOM requirement will apply to any software used in the performance of a contract. This requirement presents an onerous burden for contractors, as it is applied indiscriminately. Comparatively, the Memorandum issued by the Director of the Office of Management and Budget (OMB) on September 14, 2022, applies SBOM requirements only when an agency makes a determination that it is necessary. The proposed SBOM requirement and estimated time for its preparation do not take into account the difficulties that identifying and developing an SBOM may entail. Contractors at the prime level will need to delve into the provenance of existing software of indeterminate origin or age. They will also need to assess open source and lower-tier software for the existence of SBOMs and remediate where they are not found. In addition, some of the information may be more difficult to obtain where personnel, subcontractors, or suppliers are located outside of the United States and/or at multiple locations.

RECOMMENDATION: The SBOM requirement should be narrowed so that only contracts that are determined necessary by an agency should be subject to SBOM requirements, including alignment with those requirements already spelled out in the OMB Memorandum. Further, thought should be given more particularly on how to address issues relating to open source, aged, and other software developed in diverse or foreign locations.

3. The Scope of Requirements to Grant Full Access to CISA, the FBI, and the Contracting Agency is Overly Broad.

COMMENT: It is an onerous and, in some instances, a prohibitive requirement that a contractor must grant full access to the government—including multiple agencies and law enforcement—to applicable personnel and information and information systems in response to a reported security incident or a government-identified security incident. The term "full access" is overly broad and risks depriving the contractor and its personnel of their civil liberties, privacy rights, or the ability to narrow the scope of access. Essentially, once a cyber incident is reported, a contractor can be treated as a suspected

criminal. This is likely not the intent of the Proposed Rule and goes against the partnership that the government is attempting to establish with industry. Further, this full access is likely to interfere with the contractor's essential activities to address the incident, remediate, and perform its government contracts. Indeed, this type of full access will place greater burdens on small business contractors that have limited resources to address all the various competing needs at this critical stage. Further, the rule does not address or provide any protocols for how contractors are to handle this situation when located in different countries, with different and potentially restrictive laws on what can be disclosed and how.

RECOMMENDATION: The scope of access should be limited and narrowed to include only certain data related to an affected contract. The policy behind such access should clearly state the purpose and scope of access and that the contractor itself is not being investigated. Further, best practices or protocols should be identified to facilitate appropriate access and cooperation.

4. The Compliance Impact Analysis is Flawed and Likely to be Greatly Understated.

COMMENT: The rulemaking provides an impact analysis of compliance, which the Government admits has been developed without "precise quantifiable data." In light of events cited by the rulemaking, such as the Solar Winds and Colonial Pipeline cyber incidents, the government estimates concerning the number of contractors that will have a cyber incident, what it will take to address the incident, collect data, preserve it, and provide full cooperation and access for additional information, etc., does not reflect the real world scope, effects, and costs of a cyber incident. Depending on the size of the cyber intrusion, the scope and number of computer systems and entities affected, and the nature of the contractor (small or large, supplier or manufacturer, etc.), one can anticipate that more time will be needed to identify issues, shutdown systems, undertake remediation and forensic activities, etc., than has been estimated in the rulemaking. Thus, for example, the rulemaking's estimate of 4 hours to collect data on a cyber incident, 2 hours to submit preserved data and images, and .5 hours to share malicious code samples and artifacts vastly underestimates the time, resources, and scale necessary to report a cyber event. Care must be taken to address each of these aspects, especially in light of the risks of adverse consequences if the contract information is not properly handled, is lost, or problems in resuming performance arise.

RECOMMENDATION: The impact analysis should be revised based on specific information that should be available to the government from the incidents cited and should seek to capture input from the government contractor and the cyber incident response community. Further, steps should be undertaken to better enable and accommodate small and mid-size contractors at all tiers to have sufficient resources to address reporting requirement burdens and impacts**.**

5. Implementation and Conformity Requirements for IPv6 Should be Removed.

COMMENT: Implementation of the requirement for contractors to adopt IPv6 in their information systems, including computers, mobile devices, peripherals, and other IoT devices, and the declaration of conformity for those systems, is unrelated to the cyber-incident reporting focus of this Proposed Rule. The impact, especially to small businesses that may not have their own Chief Information Security Officer (CISO) or Chief Technology Officer (CTO) to assist with handling this activity, could be especially burdensome and has not been addressed as part of this section of the Proposed Rule.

RECOMMENDATION: Given that IPv6 is not aligned with the focus of the Proposed Rule on cyber incident reporting, it should be removed from this rulemaking and addressed separately. IPv6 is rapidly

being incorporated across the information technology environment in the course of normal technical refreshes of equipment and devices. Artificially accelerating that transition would most likely increase the cost of doing business for the government and would raise prices for goods and services the government acquires. A separate rulemaking to implement the requirements of OMB Memorandum M-21-07 would provide a better mechanism to facilitate compliance in a serial way and afford the stakeholder community the ability to assess the burdens this acceleration of conformance more effectively will impose.

6. The Rule Creates Misalignment with Compliance When Operating in an Allied or Foreign Country.

   COMMENT: The proposed rule does not address or consider and account for allied nations' or other foreign countries' requirements regarding information sharing and cyber incident reporting. For example, Directive (EU) 2022/2555 promotes cooperation, e.g., information sharing, with government entities of "third countries" (i.e., the U.S., from a European perspective). Member states and allies might choose to directly cooperate with the U.S. Directive (EU) 2022/2555 (73); however, it constrains cooperation by using the term "ensuring the Union's interests" and might interfere with full access requests, and this term leaves room for different interpretations. Further, Directive 2013/488/EU establishes that some of the information to be shared to comply with full access requests might be classified as EU-classified information (EUCI). While 2013/488/EU (b) does constrain information sharing to EU RESTRICTED, or lower, 2013/488/EU (a) explicitly allows for agreements with "Third States" (i.e., the U.S.).

   Directive (EU) 2016/943 prescribes the maintenance of confidentiality of trade secrets. Therefore, there are two categories of information, EUCI and trade secrets, which prescribe specific handling during compliance with full access requests. Directive (EU) 2016/943, however, also lists exceptions that one might apply to full access requests.

   RECOMMENDATION: The EU, through various EU directives, has a process for allowing “Third State” requests where information may include trade secrets or what can be considered EU classified information. There is no indication that the stakeholder agencies have engaged the EU to ensure that the transfer of information is not prohibitive for contractors who are prime or lower-tiered and subject to flow-down clauses. The EU would need to make a determination that such sharing is in its “interests.” Additionally, contractors and subcontractors exist in many other countries outside of EU jurisdiction, so protocols and processes for handling these types of matters need to be proposed and go through rulemaking. With the inconsistencies and concerns noted above, these issues need to be addressed before the rule goes into effect to ensure that contractors can comply.

NDIA appreciates the opportunity to comment on the Proposed Rule. Should you have any questions or wish to discuss these comments in greater detail, please contact Michael Seeds, NDIA’s Senior Director of Strategy & Policy at mseeds@ndia.org. Thank you again for the opportunity to provide NDIA’s perspectives and feedback on this proposal.

Sincerely,

National Defense Industrial Association