SUBJECT: FAR Case 2021–017
Federal Acquisition Regulation: Cyber Threat and Incident Reporting and Information Sharing

A Proposed Rule by the Defense Department, the General Services Administration, and the National Aeronautics and Space Administration on 10/03/2023

The Information Technology-Information Sharing and Analysis Center (IT-ISAC) and the IT-Sector Coordinating Council (IT-SCC) appreciate the opportunity to comment on the proposed rule FAR Case 2021-017. For over 20 years, we and our member companies have engaged with the government to improve cybersecurity, threat intelligence sharing, collaboration, and incident response. These comments reflect our continued commitment to this common cause.

One reality of cybersecurity is that the economics favor the attacker. It is more costly to defend than it is to attack. Given limited resources within industry and government, government should refrain from developing policies and regulations that would shift resources from security (detecting, preventing, mitigating attacks) to compliance. Unfortunately, it is highly likely that the proposed regulations will have such an effect.

Therefore, if industry is to divert its limited resources from security to compliance, the mandatory incident reporting program should help industry improve its security posture. As currently drafted, the regulations lack detail as to how these regulations will help increase security and resilience. Instead, the goals of the regulations seem to be to provide as much information about every possible cyber incident to the government, regardless of the severity of the incident, or the cost or benefit of exchanging such information.

For example, according to the draft regulations, the total estimated time to comply with these regulations is 10,132,041 hours. Assuming this is accurate—and in many cases the proposed regulations underestimate the time and cost it will take to implement the regulations—at a rate of $150 per hour (which is a conservative estimate in many markets), the total estimated yearly cost of compliance will be $1,519,806,150. Industry will now be diverting over $1.5 billion from security to compliance—for this one set of regulations. However, it is not clear how incurring these costs will lead to increased security. One likely outcome is that industry will price this into its costs for government customers going forward, increasing the unit cost for commercial software, computing, and cloud services, with questionable improvement for security outcomes.

While we support the goal of improving the nation's ability to identify, mitigate and respond to cyber incidents, we are concerned about several aspects of the proposed regulations. For example, we have strong concerns about the scope and scale of the proposed regulations. The definition of a reportable "security incident" is too broad and should be scoped to incidents impacting either government data or the contractor's ability to perform its mission or fulfill contractual obligations. Requiring the contractor to report "any malicious computer software" discovered anywhere on its network, even if it had no impact on data or operations, is needlessly broad.

Similarly, requiring companies to report incidents "that may have occurred" within 8 hours would require companies to report on every anomaly observed on their network. Both impose burdens to report for little or no benefit. The vast scope of the reporting requirements ensures the government will be overwhelmed with data on incidents of little importance, strategic value, or benefit to general uplift in security.

Requiring industry to share more data on routine cyber incidents that are easily resolved, do not impact the ability of a company to operate or meet its obligations under its contract, and are otherwise not material to government, will not solve the problem of sharing timely and actionable threat intelligence. This is another reason to limit the scope and scale of the reporting requirements—limiting the required reporting to consequential incidents will enable analysts to focus on a smaller amount of more meaningful information, increasing the chances they can provide analysis and intelligence that industry can then use to manage risk.

The requirement to report that an incident "may have occurred" within 8 hours is unreasonable, unworkable, and inconsistent with CIRCIA. Although the implementing regulations for CIRCIA have not been issued, CIRCIA provides companies up to 72 hours to report an incident. While the proposed regulations recognize the inconsistencies between this set of regulations and CIRCIA, it is concerning that the proposed regulations create additional, inconsistent cyber incident reporting requirements. This approach appears to be in direct contradiction to the Administration's National Cybersecurity Strategy and expressed intent to harmonize regulations. While it is not expected that this regulation harmonizes all reporting requirements, the regulations should adhere to the "First do no harm" principle.

The requirement that contractors provide government and "third parties" "full access" to their systems and people violates basic tenets of victims' rights and fairness. Based on this language, it appears that a company that reports the discovery and removal of malware on one computer somewhere in their enterprise will be forced to grant a team of government agents and government selected third parties "full access" to their networks and people. This is highly concerning.

Likewise, the proposed rule would require that contractors indemnify the government for any losses stemming from an unauthorized disclosure and give up their rights to a defense by accepting a strict liability standard for such indemnification. This runs contrary to prevailing commercial practice and seeks to use the government's buying power to impose by regulatory fiat a legal term that most commercial companies would never accept in a commercial negotiation. Given the government's knowledge about the threat environment, and its own challenges preventing unauthorized disclosures (whether from insiders or external threats), it is unreasonable for the government to insist that industry meet an impossible standard, and then shift all financial risk to contractors for such events. The government should instead continue to handle indemnification and liability issues on a contractual basis based on the particular risks and benefits of a specific procurement, enabling the parties to reach a mutually agreed upon balancing of risks. To the extent that the government wishes to seek remuneration or accountability from contractors, it should continue to use the existing legal tools at its disposal, including without limitation federal criminal statutes, civil statutes like the False Claims Act, and administrative actions. And, most importantly, the government should use its source selection authority to choose contractors who will prioritize and achieve security outcomes.

The regulations do not address how information reported to the government will be stored and protected, how access to it is limited and controlled, or how/whether the reported information is protected from the Freedom of Information Act (FOIA) requests. At a minimum, the proposed rules should indicate that sensitive or proprietary contractor information shall be withheld from public disclosure consistent with 5 U.S.C. 552(b)(4).

We also noted that the regulations include two security items that are not related to cyber incident reporting. Specifically, the regulations mandate that contractors move to IPV6 and that they develop SBOMs. Without commenting here about the security merits of these regulations, they seem out of place in a regulation focused on cyber incident reporting. We do not see the link between SBOMs, IPV6, and cyber incident reporting.

Following are more detailed comments relating to specific aspects of the proposed regulation:

1) **Scope and Flow Down Provisions**
It is important to clarify who the requirements of the proposed FAR Rule will apply to. There appears to be contradictory language that confuses the understanding of which entities are required to comply with the various provisions of the Proposed Rule.

Section 1. Background identifies the impacted entities as information technology (IT) and operational technology (OT) services providers, which is the terminology used in the Executive Order (E.O.) 14028. Section IV, however, seems to say that the proposed rule would apply if ICT is used or provided in the performance of the contract. There is a significant difference between companies that *provide* ICT and those that *use* ICT.

If the proposed rule applies to any contractor that *uses* IT or communications to provide a service to government, it essentially encompasses all contractors and subcontractors who have a computer, as opposed to the actual technology service providers as referenced in the E.O.14028. As such, there are tens of thousands of companies that will be caught up in this regulation, unbeknownst to them. No doubt most of these will be small- and medium-sized companies who can least afford the costs this will impose on them. Implementing these proposed rules could impose substantial costs beyond the company's ability to bear. Many small businesses will choose to leave the government market. Others will choose to increase their prices to cover the increased compliance costs.

Specific examples where the scope and flow down provisions are relevant include:

- A new clause in FAR 52.239–ZZ, Incident and Threat Reporting and Incident Response Requirements ***for Products or Services Containing Information and Communications Technology***, is proposed to be added as required by section 2(a) of E.O. 14028.

- The provision at 52.212–3, Offeror Representations and Certifications—Commercial Products and Commercial Services, is proposed to be revised to add definitions for information and communications technology, security incident, and security incident reports. This provision is also proposed to be updated to require

offerors to represent that they have submitted all security incident reports in a current, accurate and complete manner; and ***represent that they have required each lower-tier subcontractor under certain contracts to include the requirements of paragraph (f) of FAR clause 52.239–ZZ in their subcontract.***

- The clause at 52.212–5, Contract Terms and Conditions Required to Implement Statutes or Executive Orders—Commercial Products and Commercial Services, is proposed to be revised to add the commercial product and service usage of the new clause 52.239–ZZ, ***including flow down to subcontracts.***

- The clause at 52.244–6, Subcontracts for Commercial Products and Commercial Services, is proposed to be revised to ***add the subcontract flow down prescription for commercial product and service usage of the new clause 52.239–ZZ.***

The flow down provision also has implications for other sections of the regulations. For example, is the prime contractor responsible for reporting cyber incidents on their subcontractors, or is the subcontractor responsible for reporting the information directly? When does the eight-hour reporting requirement clock start if a subcontractor is impacted? Regardless, substantial coordination will need to take place between the prime contractor and the subcontractor, making the eight-hour timeline even more unrealistic.

Based on these provisions, we have the following questions:

- What is a "service containing" ICT technology?
- Is a company that provides toys or food to a store located on a defense base using a computer system to track orders and delivery providing a product or service "containing" ICT? Or is the scope more limited to companies that provide ICT services to the government under contract?
- Do these provisions apply only to subcontractors that provide ICT services, or any company that is part of the contract? For example, does the flow down provision apply to subcontractors who do not provide ICT services under a contract, even though the contractor provides ICT services?

Without understanding the intended scope of who is covered, companies would not know which of their subcontractors they would need to include as part of their compliance.

2) **Requirement to provide Software Bill of Materials (SBOM)**
As previously noted, the requirement for companies that provide software to government to maintain SBOMs seems out of place for a regulation on cyber incident reporting. We also are concerned about this provision for multiple reasons. Primary among them is that it is not clear the degree to which this initiative is aligned with other E.O. 14028 software security requirements, including finalization of software supply chain security self-attestations associated with OMB Memo 22-18.

Also, meeting such a requirement would be difficult to achieve, or indeed be cost prohibitive, for many organizations. Despite the many years SBOMs have been under development, there remain significant challenges in consistently producing them at scale. As one example, there currently is not a common format for SBOMs. The more formats there are, the more expensive it is to do at scale. While meeting this requirement would be challenging for organizations of all sizes, these burdens would be greatest on smaller organizations with fewer resources. This could create downstream market impacts as smaller entities are unable to compete.

3) **CISA Engagement Services and Access to Contractor Information and Information Systems**

The proposed rule requires companies that report an incident, or if the company has been identified by government as a victim, to provide government and "third parties," at the request of government, unfettered and indefinite access to the victim company's network and employees. As previously discussed, this section raises fundamental questions about victim's rights. There are long standing legal processes and procedures that the government can use to gain access to evidence. These processes should not be discarded simply because a company is a victim of cybercrime.

Under this proposal the government can gain "full access"—not access only as needed to investigate a specific incident, but access to everything—for any incident that has been reported. At the very least, this provision needs to be limited to severe incidents, and access should be limited to only what is required to investigate the incident. Further, access should be time-limited, and any extension beyond that limit would need the concurrence of the victim company.

There are also concerns that this requirement will hinder the company's timely, efficient, and successful response to the incident. In case of an incident, a company will first utilize its internal resources. If special assistance is required, it will bring a third-party team under contract. As such, the company will be managing the incident while trying to comply with various government reporting requirements. This will be extremely difficult for large enterprises and almost impossible for smaller ones.

Taken together, there is a concern about the lack of boundaries on this access, coupled with the likelihood that other governments will ask for the same privileges. For example, does "systems" include all systems (whether or not they were part of an incident) such as, say, source code repositories? If so, that is a grave risk to intellectual property. If something is inadvertently leaked, it can affect patentability—not to mention others can potentially steal the IP if they have access to these systems. It's not just a matter of the inconvenience of having a slew of government agents and third parties disrupting your response to an incident. Risking the loss of your IP is even worse.

It is unclear what benefit is achieved through this provision. Creating an adversarial relationship between the victim company and government agencies will not lead to better outcomes. We believe the goals of this provision can be achieved through partnership between the victim company and appropriate government agencies.

Companies already retain the option to ask for assistance if needed. There also is the option for the company to provide the government with the incident report provided by their third party. CISA often compliments victim companies for engaging with them in incident response.

Finally, the below provision in the CISA Engagement Services section that appears to limit the ability of a victim company to deploy remediations would be highly problematic.

> *"It is expected that any action taken in response to such recommendations [from CISA] would only be taken after consultation between the contractor and the contracting agency, including both the requiring activity and the contracting officer."*

Limiting a company's ability to administer immediate remediations could potentially cause more damage and prevent the timely deployment of mitigations.

Taken together, this section raises several obvious questions that need to be clarified with further explanation. For example:

- Will the government be dictating to a victim company what actions it can or cannot take to remediate an incident on their own network?
- How is "full access" defined?
- How long after an incident is reported is the government able to demand access to a victim's network? Days? Weeks? Months?
- For how long must a company provide full access?
- Who—the victim company, CISA, the FBI, the Contracting Agency—is responsible for incident remediation when government demands full access?
- Who will be the authority to justify and approve such an engagement?
- Does the contractor or subcontractor have the option to object to such an engagement initiated by CISA?
- Can the victim company request a third-party provider other than the one the government is providing?
- Will CISA/FBI/Contracting agency be required to provide a justification or specific purpose or cause for initiating such an engagement with a contractor or subcontractor?
- During the course of such an engagement, how will the information collected be gathered, stored and secured?
- Who will have access to such information? Will such information be shared with other federal departments/agencies?
- Will the information gathered by CISA or other federal departments and agencies be subject to FOIA, or what legal provisions will provide protection or an exemption to disclosure under FOIA requirements?
- How will such an engagement interact with third-party or managed service providers, should that be the practice for the targeted contractor or subcontractor?
- Who will have the final say on any remediation steps or actions?

4) Security Incident Reporting Harmonization

As previously noted, the regulations propose an additional timeframe for reporting cyber incidents. This regulation contradicts the 72-hour baseline contained in the CIRCIA. We recommend regulations requiring incident reporting maintain Congressional intent from CIRCIA, and a key element of the Administration's National Cybersecurity Strategy and do not establish yet another standard.

The proposed rule requires contractors 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."

Requiring companies to investigate and report that an event "may have occurred" is unrealistic and counterproductive to security. Everyday security teams investigate security incidents that "may have occurred." Most of these, thankfully, are something other than a cybersecurity incident. Requiring contractors to report on every potential indicator they investigate does not benefit either industry or government. For industry, it will divert resources from security and other core business and security functions for no meaningful purpose, limiting its ability to identify incidents that have actually occurred and mitigate them in a timely manner. In return, the government will receive a lot of meaningless noise.

If this requirement remains, CISA will be quickly overrun with unverified, outdated indicators, and with hundreds, potentially thousands, of reports each day that an incident "may" have occurred. None of this will improve cybersecurity. The regulations seem to be scoped at giving the government as many indicators as possible, rather than creating a framework in which government can conduct valuable analysis on confirmed, meaningful incidents.

In addition, the eight-hour timeline is unreasonable without a clear benefit. Incident reporting requires significant internal coordination for an event on a company's network, let alone coordinating across subcontractors. For example, suppose an analyst at a 24x7 SOC has an indication at 2:00 AM ET that an incident "may have occurred." It will be at least six hours before the leadership team engaged in reporting the incident will be available—if the team is located on the east coast. It is likely to be nine hours before that process can be initiated for a company on the west coast.

Likewise, suppose a Managed Security Services Provider identifies a potential incident on a small business customer network. Investigating the incident, contacting the customer, and coordinating with the customer on incident response will be a time-consuming and stressful endeavor, especially for the small business. The small business will then either need to notify the prime contractor or report it directly. Doing all of this in eight hours is not realistic in most circumstances.

Given the ubiquity of ICT in products and services, contractors may offer products and services to the government that are subject to additional incident reporting requirements imposed by other contracts or regulatory regimes. When the same underlying systems are subject to inconsistent or contradictory incident reporting requirements, companies may focus more on compliance than on security. Similar results may occur when such requirements are duplicative but enforced differently by different counterparties or regulators. This may eventually lead to organizations passing higher costs on to customers, including the government. This resource diversion could also lead to weaker security measures or longer undetected security incidents. As such, we urge that reporting be limited to actual incidents that impact government data, government functions, or the ability of the victim company to provide its contracted services.

In addition, any reporting timeline should consider:

- Why an eight-hour reporting requirement?
- When does the clock begin for the eight-hour reporting requirement?
- Are prime contractors expected to report on incidents of their subcontractors, or are subcontractors expected to report incidents directly to the government?
- Given the flow down requirements for subcontractors, how is the timeline established throughout the supply chain and subcontractor regime, particularly given the fact that many subcontractors are small- and medium-sized businesses and may not have full-time staff allocated to monitoring indicators?
- How is an ongoing and continuing 72-hour follow up reporting submission timeline determined to be required until there is evidence that the purported event is fully and completely resolved? Depending on the nature of the incident, this could be an extended period of time requiring an ongoing commitment of resources in order to comply.
- Relatedly, how does the Proposed Rule define "*completed all eradication or remediation activities,"* and who determines this?

5) **Expected Impact of the Proposed Rule**

Executive Order (E.O.) 14028, which authorizes the proposed regulations, tasked the government to develop and implement mandatory cyber incident reporting rules for "IT and OT service providers." Instead, according to the draft regulations, *"This proposed rule will impact all contractors awarded contracts where ICT is used or provided in the performance of the contract."* This is a significant expansion of scope, without explanation.

One consequence of this is that companies that were not the focus of the E.O. are not aware these regulations impact them. This will limit the ability of government to receive feedback from potentially impacted companies, many of which are small- and medium- sized enterprises. This concern is enhanced by the fact that not even the government can quantify who in industry is impacted by this regulation. The government can only "assume" that 75% of all contracts "include some ICT."

Using the government's estimates demonstrates both the compliance challenges and the need to scope the reporting requirements. By the government's own admission, this regulation can impact over 70,000 entities, 46,000 of whom are small businesses. Each of these entities are now expected to establish a reporting regime that will enable them to report, within eight hours, indicators that a cyber incident "may have occurred" and to participate in AIS so that it can share with CISA indicators not related to a reportable incident. Based on our discussions with businesses across various industries that leverage IT to provide services contracted to the government, we worry that most companies that will be impacted by this regulation are not aware of it, and that the government does not fully understand the costs and compliance challenges industry face. Many companies will choose to leave the government market, potentially depriving government of critical expertise, services, and products.

6) **Subscribing to CISA's AIS Program**

The proposed regulations require contractors to subscribe to CISA's AIS program or to participate in a Sector Specific Information Sharing and Analysis Center (ISAC), or other information sharing organization. We appreciate the flexibility that companies can choose. However, we would like to note that AIS and participation in a sector-specific ISAC have two totally different value propositions. AIS is focused on sharing indicators at scale, while ISACs provide actionable threat intelligence that enables companies to manage a wide range of risks.

We have long been supportive of AIS. However, AIS also has substantial problems that were catalogued by a 2022 DHS Inspector General report. In a December 2023 announcement, DHS itself conceded on the need to revamp and modernize AIS and announced a multi-year effort to revamp the program. As such, it is uncertain what the AIS program will entail in the future.

In addition, many entities do not leverage the automated technology that is required to share or receive indicators through AIS. This is true for large enterprises, but especially true for small- and medium-sized enterprises. According to CISA, leveraging AIS requires companies to build or buy specialized capabilities to participate. Even if a small business invested in the capability to consume AIS feeds, sending these businesses AIS indicators would have no value in most cases.

In contrast, participation in sector-specific ISACs enables companies to receive indicators shared through the AIS program, as well as trusted, vetted, vendor-neutral analysis. It provides the opportunity for companies to engage with analysts from peer companies who are addressing the same security challenges and threats. ISACs provide flexibility to meet a wide range of needs from the diverse set of member companies. Companies that want to consume and share indicators have the platform to do so. At the same time, companies also receive threat analysis, coupled with specific recommendations to mitigate risks.

For these reasons—the current challenges with AIS, the uncertainty of the program, the fact that most contractors do not have the ability to consume AIS feeds, and the enhanced value ISACs provide in risk management—we support the flexibility that is provided in the proposed regulations.

7) **Regulator Familiarization and Public Burden**
(f) 52.239–ZZ, paragraph (c)(4), for contractors to support incident response by providing to the government and any third party authorized assessor all incident and damage assessment information identified in clause paragraphs (c)(1)–(3), if the government elects to conduct an incident or damage assessment.

We have discussed various aspects of the third-party requirement previously. However, we would like to raise the point here that the victim company should have a right to request an alternate third-party assessor, rather than be expected to accept any third party the government imposes. For example, what if the victim company had a previous engagement with the third-party assessor that did not go well? What if the third-party assessor is a direct competitor? What if the victim company already has a trusted relationship with a third-party that is not the one that the government is engaging with? Common courtesy and fairness dictate that the victim company should have the ability to object to a government-appointed third-party.

We have additional, specific areas of clarity we are seeking related to this section:

- Please clarify the definition of a "3rd party authorized assessor" and what parties would qualify for such a designation on behalf of the government.
- Please clarify the requirements for any designated "3rd party authorized assessor" for the collection, storage, and security of any information provided, and who that information will be authorized to be shared with.
- Please clarify whether the information collected by a non-government "3rd party authorized assessor" related to a security incident and damage assessment would be subject to the provisions of FOIA, or whether an exemption is authorized by law.

8) **Cost and Public Burden**
We are not confident in the estimated cost of compliance. In one example, the government estimates it will take on average 80 hours to build and maintain an SBOM. Given the experience of many companies that have attempted this, and the efforts to build and maintain SBOMs have been ongoing for multiple years this seems unrealistic. Even if the estimate that an SBOM for a product can be built in 80 hours was correct, companies often use multiple products in government contracts.

Further, assuming the estimate that it will take four hours to report an initial incident or potential incident is accurate (our experience is that this estimate is way too low), there are two points to be raised. The first is that even this estimate reveals how unreasonable the eight hour timeline is -- half of the eight hours are estimated to be spent on compliance. That leaves only four hours of investigation and remediation.

The second is that the estimate provided does not account for the subsequent updates that are due every 72 hours for as long as the incident is ongoing.

Also, the "Sharing Threat Indicators" estimate does not appear to consider the cost to buy or build the capabilities that are required to subscribe to AIS. As already noted, AIS is not the right solution for many companies who have no way to use the indicators.

Finally, the regulations estimate that only "4 percent of the entities will have a reportable cyber incident for which this information collection activity applies." Given that the regulations require reporting "incidents that may have occurred," we expect the vast majority of contractors would be impacted by this reporting requirement.

The IT-ISAC and IT-SCC appreciate the opportunity to present these thoughts. We share the government's goal of improving cybersecurity within industry and government. We remain committed to voluntary collaboration with our industry and government partners and look forward to continued engagement on these important topics.

Thank you for your consideration.