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 Food and Agriculture-Information Sharing and Analysis Center (Food and Ag-ISAC) appreciates the opportunity to comment on the Federal Acquisition Regulation (FAR) Proposed Rule: Cyber Threat and Incident Reporting and Information Sharing. The Food and Ag-ISAC provides threat intelligence, analysis, and effective security practices that help food and agriculture companies detect attacks, respond to incidents, and share indicators so they can better protect themselves and manage risks to their companies and the sector. Our member companies span the food supply chain and include companies that provide product and food related services to the federal government.

We have studied the proposed regulations in detail and have several concerns. These include:

- **Requiring the Implementation of IPV6 and Subscribing to AIS**

  It is not clear how requiring implementation of IPV6 is related to cyber incident reporting. In addition, there is no technical reason for food and agriculture companies to implement IPV6 in the current environment. Companies would incur significant costs to make this migration and there is no greater public gain for them to do so.

  Similarly, requiring companies that do not participate in Information Sharing and Analysis Centers (ISACs) to subscribe in AIS will likewise increase costs for little public gain. There are multiple shortcomings with the AIS program. CISA concedes this and recently announced its intent to revamp the program. It is unclear what changes will be made and what value will be gained. However, implementing automated sharing capabilities within larger enterprises can be challenging and costly. The challenge is even greater for smaller enterprises. Given the known costs of implementing AIS and the uncertainty of the program, this requirement is imprudent.

  In contrast, active participation in sector-specific ISACs is known to return tangible value to companies. For example, the Food and Ag-ISAC serves as a cost-effective force multiplier to the security teams of our member companies. In addition to automated indicator sharing and collaborative analysis among members, the Food and Ag-ISAC connects government to industry-specific subject matter experts, provides a forum to consider dependencies within the sector, and facilitates engagement with other critical infrastructure ISACs for cross-sector sharing and interdependency analysis.

- **Proposed Regulations Go Beyond the Scope of Executive Order (E.O) 14208**

  Executive Order 14208 was focused on "IT and OT service providers" and "information and communications technology (ICT) service providers". The proposed regulations apply to "products or services ***CONTAINING*** information and communications technology". FAR 2021-07 is a significant change and captures any company that uses a computer. This change in scope means that any company that is a prime or subcontractor on a government contract will be required to report any "potential" cyber incident.

  The impact of this across the business community cannot be overstated. Tens of thousands of companies who do not provide IT, OT or communications services are now included as "ICT service providers." Many companies, especially small businesses, lack the resources necessary to build the compliance structures to adhere to these regulations. Some companies might absorb the costs, but many will increase the price of their service to recover costs. Others will decide the cost of compliance is too great and withdraw from the government market, depriving the government of a vital product or service.

  To put this in context, an Executive Order designed for companies that provide ICT and OT services to government will now be binding on food and agriculture companies such as:

  - Transportation companies that deliver food and products to commissaries on military bases and other government facilities.
  - Grocery stores and restaurants with contracts to operate in military bases.
  - Companies that provide food and beverages to any federal government entity.
  - Companies that provide catering services to any federal government entity or office.

  We urge that the regulations be scoped to the original intent of the Executive Order – "IT, OT, and ICT service providers". Scoping the regulations beyond this, to any contractor who uses these services, will have costs that go well beyond any perceived government benefit and risks potential disruptions to the delivery of critical products and services.

- **Flow Down Provisions Risks**

  The flow down provision risks including companies who do not consider themselves to be contractors and is concerning for several reasons. Beyond the obvious point that many suppliers in the food and agriculture industry are small- and medium-sized enterprises that likely do not have the resources to comply with many aspects of the proposed regulations, the reality is that many companies are not aware that their product is provided to the federal government. Companies that provide product in bulk to customers are not always aware of the final destination of the product.

  For example, a company contracted to provide fuel to Company A, does not always know if Company A is using that fuel for federal contracts. The company is simply fulfilling an order to Company A. In this case, the supplying company is a subcontractor without knowing it. This example applies to a range of products within the industry. A family farm that provides grain to a company, who then uses that grain in product that is sold to the federal government, could be considered a subcontractor.

In addition to the ambiguity around responsibility for reporting in a prime/subcontractor arrangement, there would have to be a pre-established obligation between companies and subcontractors establishing these new requirements. This would require all contracts be amended to include these requirements, which will be a significant burden - especially for larger organizations where it may take thousands or tens of thousands of hours to negotiate and amend around the new requirements. This could also result in subcontractors no longer wanting to engage in business with these companies, causing selection of alternate subcontractors that could result in higher costs of services and/or goods that would have to be passed along to consumers or the government.

Therefore, we request that the regulations scope as to what is considered to be a subcontractor, and/or somehow limit flow-down provisions to avoid unintentionally including companies without federal contracts. In addition, the final rule should make it clear that it is the prime contractor's responsibility to notify subcontractors that the product/service they are providing will be used in completion of a federal contract. Finally, we suggest that subcontractors should not be held liable for noncompliance if the prime contractor did not properly disclose the use of the products and/or services being purchased.

- **Eight Hour Incident Reporting Requirement**

We would like to highlight two concerns with this provision. The first is that eight hours is unreasonably short, creates compliance challenges, and creates a requirement that is contrary to CIRCIA, which was passed by Congress and signed by the President. Understanding and reporting a cyber incident is a complex task that involves multiple departments, potentially across several business units. It is not clear as to why the regulations propose eight hours, or why the 72 hour timeframe contained in CIRCIA is not sufficient.

Relatedly, the same provision contains a requirement that the company "update the submission every 72 hours thereafter until the Contractor, the agency, and/or any investigating agencies have completed all eradication or remediation activities." Depending on the incident, this could potentially take months to resolve. Who determines when an event has been completely eradicated or remediated? The regulations do not detail the value that is gained by requiring companies to provide updates every 72 hours for months. Such a requirement seems only to divert critical resources from incident response and recovery.

The second concern relates to the requirement that reporting is not limited to actual incidents, but to those that "may have occurred." Our members investigate potential security incidents each day. Thankfully, the vast majority of these are not actual cyber incidents. Requiring the reporting of non-incidents does not add value to either industry or government. From an industry perspective, it diverts limited resources from actual security work. From the government perspective, it would waste resources analyzing non incidents, rather than focusing on actual incidents.

Therefore, we recommend that the reporting be scoped to include actual, confirmed incidents that impact the contractor's ability to provide its contractual product or service, and to those that impact government data hosted by the contractor.

- **Access to Contractor Information and Information Systems**

  We are extremely concerned with the requirement that victim companies grant the government "full access" to their systems and employees if they report a cyber incident or if the government suspects they were victims of a cyber incident. We are not aware of another instance in which the victim of a crime must grant law-enforcement, government agencies, and government chosen third-parties unlimited access to their property and employees. Our experience is that victim companies most often are willing to cooperate with law-enforcement. In the rare instance in which a company is not cooperative, the government has a range of legal and investigative tools at its disposal. When a company is a victim of a cybercrime, they expect law enforcement to be a trusted, confidential, and compassionate partner in the investigation. This requirement flips that relationship and creates an adversarial relationship between the victim company and government responders.

  The provision that enables government-appointed third parties to also have unlimited access is equally concerning. What if the victim company does not trust the government-appointed third party? What if they are business competitors? What if they had previous relationships that were not satisfactory to the victim company? What if the victim company is already engaged with a third party? There does not appear to be any recourse or means for the victim company to object to the government-appointed third party.

  Consider this provision in action. A company finds a piece of malware on a portion of its network that is segmented from the network that supports any government contract. There is no impact to the company's ability to perform the government contract, and there is no impact to the confidentiality, integrity, or availability of any government data. The company reports this incident to CISA. CISA, the FBI and the contracting agency can now demand "full access" to the company's network and bring in a third party of its choice. The victim has no control over any of this.

  To implement this provision, companies would have to have two fully staffed and dedicated incident response teams. One would be required to manage the government and its third-party responder. The other would be required to manage the actual incident itself. Taken as a whole, this provision will hinder the ability for the victim company to effectively respond to, recover from, and remediate the incident.

- **Information Disclosure**

  The regulation does not detail how reported information, or information collected by the government through incident response, can be shared within government or industry, and is protected from public disclosure. The information reported under this regulation can contain sensitive and proprietary information. Additionally, the government and its designated third parties may obtain additional information about the victim company as part of its response to an incident. Protecting this information from public disclosure and ensuring the privacy of the victim company is essential. In addition, the regulations do not address issues such as:
    - Whether reported information is protected from disclosure under the Freedom of Information Act (FOIA). CIRCIA protects such information from FOIA disclosures. Will such protections be applied to these regulations?
    - How the government will handle, store, and protect information reported to it or that it collects as part of its investigation, and who will have access to it?

- How the government-appointed third-party incident responders can use the information they collect in their response. What government agencies can they share information with? Are they permitted to use or resell the information in their products or services?
- How government agencies will re-share information with industry. What obligations are on government agencies to provide threat intelligence from reported incidents to industry at large? Who is responsible for doing this? How will the confidentiality of the victim company be protected throughout this process?

The Food and Ag-ISAC appreciates the opportunity to contribute, and thanks you for your consideration of our comments.