CSP-AB ITI NDIA PSC PROFESSIONAL SERVICES COUNCIL SIIA

January 14, 2025

Sent via the Federal eRulemaking Portal: https://www.regulations.gov

Ms. Heather Kitchens
OUSD(A&S) DPC/DARS
3060 Defense Pentagon
Washington, DC 20301-3060

Multi-association comments regarding DFARS Case 2018–D064 Disclosure of Information Regarding Foreign Obligations

The undersigned associations appreciate the opportunity to comment on the proposed rulemaking associated with DFARS Case 2018-D064 Disclosure of Information Regarding Foreign Obligations ("the Rule"). Our members include many of the most innovative traditional and non-traditional defense contractors that support the Department of Defense (DoD) in its mission delivery through the provision of technology solutions and associated services.

Section 1655 of the National Defense Authorization Act (NDAA) for Fiscal Year 2019 ("Sec. 1655") called for the disclosure of information regarding contractors' foreign obligations. The DoD has taken the position that the proposed clause should apply to commercial products, including Commercially Available Off-the-Shelf (COTS) products. We question whether the decision to apply the disclosure requirements to commercial products is truly in the Department's best interest. We also believe that there are opportunities to align business practices to support compliance while acknowledging the complexity of the global market.

The Rule proposes Sections 252.239-70YY and 252.239-70ZZ to implement the disclosures required by Section 1655(a) for offerors and contractors, respectively. In doing so, the proposed regulatory language exceeds the legislative requirements—and thereby DoD's delegated authority—by expanding the scope of the disclosure requirements to scenarios that were not intended to be covered by the underlying legislation.

While Sec. 1655 delineates different disclosure requirements for commercial and non-commercial products, the Rule, as proposed, conflates the disclosure requirements for non-commercial products and commercial products as defined in Sec. 1655(a)(1) and Sec. 1655(a)(2) respectively. This expands the scope of covered products, systems, and services to a futile degree. COTS products are intended for broad use by commercial entities and are not exclusively designed for government use cases. Subjecting effectively all products produced by the defense industrial base to these disclosure requirements will create countless false positives. Simultaneously, it will raise the barriers to market entry and exacerbate the current decline in innovative market participants. This erases any benefit to risk management, contradicts the Department's objective to build and foster a resilient and innovative defense industrial base, reduces operational efficiency and complicates successful mission delivery.

To prevent these undesirable consequences, we recommend that the proposed rule be updated to align with the underlying statutory requirement. To that end, we recommend a complete rewrite of the proposed amendments to Part 252-Solicitation Provisions and Contract Clauses to bring it into alignment with Sec. 1655. Below, we provide a summary of our concerns as well as recommendations on how to address these concerns. Specifically, we recommend that the Department:

- Limit the disclosure requirements pursuant to Sec. 1655(a)(1) to non-commercial products, systems, and services
- Do not introduce additional requirements for the acquisition of commercial products and services under FAR Part 12 to preserve the nature of commercial products and services
- Limit disclosure requirements pursuant to Sec. 1655(a)(1) to instances of governmental review
- Limit Disclosure Requirements pursuant to Sec. 1655(a)(2) to foreign persons acting on behalf of a foreign government of concern as identified by Sec. 1654 list of countries
- Exempt products, systems, and services from disclosure requirements if they are subjected to a de minimis disclosure under restricted access conditions
- Edit disclosure requirements pursuant to Sec. 1655(a)(3) for clarity
- Limit disclosure requirements to the time after contract award
- Revise the effective date to meet Congressional intent
- Tie disclosure requirements to vendors' actual knowledge
- Expand OSS exemption and apply it to OSS components embedded within end products
- Limit Data Access to Federal Authorities with a Need to Know
- Strike subcontractor flow-down provisions
- Strike representation and attestation requirements.
- Define key terms

We thank you for your consideration of our recommendations. If you have any follow up questions, please reach out to Leopold Wildenauer, ITI's Director of Public Sector Policy, at lwildenauer@itic.org.

Kind regards,

Cloud Service Providers – Advisory Board (CSP-AB)

Information Technology Industry Council (ITI)

National Defense Industrial Association (NDIA)

Professional Services Council (PSC)

Software & Information Industry Association (SIIA)

Limit the disclosure requirements pursuant to Sec. 1655(a)(1) to non-commercial products, systems, and services

The decision to consider commercial products as in scope for all disclosures in the Rule is contrary to the statutory text. Sec. 1655(a)(1) explicitly[1] limits disclosure requirements to non-commercial products, systems, and services developed for the Department. Consequently, the regulatory implementation of Sec. 1655(a)(1) must not apply to any commercial products, including COTS.

As proposed, Sections 252.239-70YY(c)(1)(i) and 252.239-70ZZ(c)(1)(i) would expand the scope of disclosures pursuant to Sec. 1655(a)(1) from "non-commercial products" to "any product, system, or service that DoD is using or intends to use." However, the underlying statute does not support such a scope expansion. We urge the Department to limit the disclosure requirements pursuant to Sec. 1655(a)(1) to non-commercial products, systems, and services as was intended by Congress.

Do not introduce additional requirements for the acquisition of commercial products and services under FAR Part 12 to preserve the nature of commercial products and services

The government typically acquires commercial products and services under FAR Part 12. The intent of FAR Part 12 is to allow the government to purchase commercial products and services that are sold or licensed to the commercial marketplace. This allows the government to acquire such products based on commercial terms, including pricing. When the Department introduces additional requirements for the acquisition of commercial products and services, this marks a deviation from what is being implemented by FAR Part 12.

As it currently stands, it appears that the Rule changes the scope of FAR Part 12. If the government wants to engage in the commercial marketplace, especially concerning COTS products, the expectation should be to acquire the same products that are sold/licensed to the general public, without meeting special requirements. COTS products become non-commercial when special requirements are mandated by the government. Characteristics of commercial products, such as pricing, would be affected by such requirements. The export regulations dictate who can purchase such

[1] Sec. 1655(a)(1) "Whether, and if so, when, within five years before or at any time after the date of the enactment of this Act, the person has allowed a foreign government to review the code of a **non-commercial product, system, or service** developed for the Department, or whether the person is under any obligation to allow a foreign person or government to review the code of a **non-commercial product, system, or service** developed for the Department as a condition of entering into an agreement for sale or other transaction with a foreign government or with a foreign person on behalf of such a government."

products. Otherwise, commercial companies are at liberty to sell or license their products globally.

Limit disclosure requirements pursuant to Sec. 1655(a)(1) to instances of governmental review

Sec. 1655(a)(1) delineates two scenarios under which disclosure is required. The first applies when a foreign government has reviewed the code for a covered non-commercial product. The second applies when a code review is required as a condition of conducting business with a foreign government or a person acting on behalf of such a government. Neither statutory scenario applies to code reviews by foreign persons, especially if they occur as part of low-risk customary commercial practices.

As proposed, the Rule would force traditional and non-traditional defense contractors who develop software for the global market to file a disclosure for virtually every product, service, or system acquired by the Department. In fact, it would punish commercial technology companies who wish to sell their innovative software to the government but have US-based staff with various immigration statuses.

Requiring the disclosure of source code reviews by any foreign person would not enhance US national security nor would it meet legislative intent. We believe that the proposed expansion of the statutory requirements creates significant burdens and may severely limit the software products available to DoD, all while having only a questionable benefit for security. Moreover, the proposed rule may expose contractors to legal action abroad as prohibitions on the disclosure of source code reviews, trade agreement provisions, and privacy laws all pose barriers to compliance with the regulation as currently proposed.

We recommend that the Rule be updated to limit the disclosure requirements for covered non-commercial products to reviews by foreign governments. Source code reviews by foreign individuals should not be brought into scope for Sec. 1655(a)(1) disclosures, especially when they occur as part of low-risk customary commercial practices. Additionally, the Rule should provide companies with guidance on how to comply with the proposed requirements in accordance with existing obligations under international law. We believe that these measures will avoid harm to US economic security, minimize international legal risk, and improve government efficiency all while being consistent with statutory intent.

Limit Disclosure Requirements pursuant to Sec. 1655(a)(2) to foreign persons acting on behalf of a foreign government of concern as identified by Sec. 1654 list of countries

Consistent with statutory intent, the implementation of the disclosure requirements pursuant to Sec. 1655(a)(2) should be limited to instances when the source code has been reviewed by a government of concern or an individual acting on behalf of such government. Again, this notification trigger should not be applied to Sec. 1655(a)(1) disclosures.

The disclosure under Sec. 1655(a)(2) covers whether "the person has allowed a foreign government listed in Sec. 1654 to review the source code of a product, system, or service that the Department is using or intends to use." The disclosure under Section 1655(a)(2) also covers whether the person "is under any obligation to allow a foreign person or government to review the source code of a product, system, or service that the Department is using or intends to use as a condition of entering into an agreement for sale or other transaction with a foreign government or with a foreign person on behalf of such a government."

As proposed, the implementing language completely ignores and removes the important text of Sec. 1655(a)(2), which limits the scope of this disclosure requirement to cases involving "a foreign government listed in Section 1654." This, again, exceeds statutory intent, reduces operational efficiency, raises costs, and yields no actionable risk intelligence.

We recommend that the Rule be updated to limit disclosure requirements pursuant to Sec. 1655(a)(2) to source code reviews by governments of concern as identified in the list pursuant to Sec. 1654 or individuals acting on their behalf. Such a list should be at the heart of regulatory implementation, narrowly tailored, and rooted in demonstrable threats to U.S. government supply chains. Further, contractors will require additional guidance on how to access the most up-to-date version of the list pursuant to Sec. 1654. Additionally, the requirement should distinguish between, for example, an independent testing laboratory conducting a code review on behalf of a foreign government and a non-government-affiliated foreign person conducting code review for quality assurance during software development on behalf of a vendor or as part of a widely used industry-accepted accreditation or certification process.

Exempt products, systems, and services from disclosure requirements if they are subjected to a *de minimis* disclosure under restricted access conditions

In the Joint Explanatory Statement accompanying the FY19 NDAA, conferees noted that the Secretary of Defense should "exempt from this requirement any product, system, or service if: (1) its source code has been exported pursuant to a license or license exception granted under the Export Administration Regulations (15 C.F.R. §§ 730774); (2) it is not itself, and is not a component of, a National Security System; (3) it is not a cybersecurity tool, system, or application or does not have a built-in cybersecurity tool, system, or application; or (4) it is subjected only to a *de minimis* disclosure under restricted access conditions, as defined by the Secretary." Conferees also encouraged the Secretary to allow for products, services, and systems to be exempted from disclosure requirements in Section 1655 if they are "subjected only to a *de minimis* disclosure under restricted access conditions, as defined by the Secretary."

We recommend the establishment of reasonable criteria for a *de minimis* review to prioritize the most high-risk code review activities, thereby minimizing unnecessary processes and compliance requirements in instances where compromise of a product, service, or system is highly unlikely. We recommend applying exemptions to the disclosure requirements for *de minimis* code reviews that meet any of the following criteria:

- Access to code is provided in the ordinary course of business (e.g., to ensure technology interoperability, updates, bug fixes, or software development kits);
- The code review involves disclosure of less than two percent of the source code of the subject product, system, or service;
- The code subject to the code review is identified by an automated scanning tool from an internationally recognized provider of such tools;
- The code review and related analysis are conducted at a vendor-controlled facility or at an internationally accredited independent laboratory facility located outside a country identified in the Countries of Particular Concern list created under Section 1654;
- Automated code scanning and analysis conducted in relation to the code review are conducted by the vendor or by an independent and internationally recognized third party in the presence of the vendor;
- The code review involves no recording devices;
- Parties receive a paper summary of results, and no other materials associated with the code review are provided or permitted to leave the facility; and
- The code review complies with any relevant internationally recognized standards.

Edit disclosure requirements pursuant to Sec. 1655(a)(3) for clarity

Disclosures under Section 1655(a)(3) cover whether the person holds or has sought to hold a license pursuant to the EAR, ITAR, or successor regulations "for information technology products, components, software, or services that contain code custom-developed for the non-commercial product, system, or service the Department is using or intends to use." Non-commercial products are defined by Sec. 1655(h)(5).

We recommend that the Rule be edited for clarity to apply the NDAA-provided definition of "non-commercial product, system, or service" as provided by Sec. 1655(h)(5). Moreover, we recommend that the Department clarify the timeline for this section. Due to the dynamic nature of software development, we believe a reporting period of 1 year would best reflect EAR and ITAR licenses.

Limit disclosure requirements to the time after contract award

Sec.1655(c) establishes the procurement requirements for disclosures pursuant to Sec.1655(a). The section does not call for the preaward disclosures described in 252.239-70YY and clearly states that all disclosure requirements should apply after contract award:

> (c) PROCUREMENT.—Procurement contracts for covered products or systems shall include a clause requiring the information contained in subsection (a) **be disclosed during the period of the contract** if an entity becomes aware of information requiring disclosure required pursuant to such subsection, including any mitigation measures taken or anticipated. [emphasis added]

However, proposed clause 252.239–70YY Preaward Disclosure of Foreign Obligations—Representation establishes the disclosure requirements as selection criteria for contract award and requires completion of the foreign obligation disclosures prior to exercising an option.

We recommend that the requirements be focused on the postaward disclosure of foreign obligations. Sec. 1655(c) does not call for the proposed preaward disclosures of foreign obligations. Removing section 252.239-70YY would bring the implementing rulemaking back into line with the statutory intent.

Revise the effective date to meet Congressional intent

The proposed rule calls for disclosures of whether, and if so, when, at any time after August 12, 2013, the offeror has allowed a foreign person or foreign government to review the source code for any product, system, or service that DoD is using or intends to use, or the computer code of any other than commercial product, system, or service developed for DoD. This suggested lookback period is longer than the standard norm for such a process and exceeds the reasonable inquiry standard found in FAR 52.204-24 and FAR 52.204-25 for representations regarding certain telecommunications and video surveillance services or equipment.

As proposed, the Rule would require vendors to retroactively report reviews for at least twelve years. It is not commercially reasonable to expect that vendors will have this level of detail about transactions that date back to August 12, 2013, which would include data about (1) which code was shared with any foreign governments or any foreign persons; (2) when such code was shared; and (3) whether that particular code is found in products (including commercial products) that DoD is using or intends to use. This is particularly true if the requirement for disclosure of source code in Commercial and COTS products is not tied to the Section 1654 list as specified in Section 1655.

We recommend that the 5-year statutory period run from the enactment of the DFARS clause instead of the enactment of statute. We also recommend that DoD update the rule to include a cost-impact analysis of the proposed requirements on contractors. Further, we recommend that the rule clarify that contractors are only expected to make reasonable inquiries designed to uncover information in their possession about sharing of code with foreign governments and about whether such code is in products that DoD uses or intends to use. Additionally, we recommend that Rule clarify that the notification requirements apply only in cases where the offeror was under a contractual obligation to allow source code review at any time after August 12, 2013, and is still under such obligation at the time the offeror discloses the obligation to the Government. Moreover, the rule should contain a secure mechanism to allow contractors to ask and receive feedback from DoD to identify which of the contractor's commercial products and version numbers DoD is using or intends to use, to help enable the contractor to make accurate disclosures under the rule.

Tie disclosure requirements to vendors' actual knowledge

The proposed Rule provides no flexibility for companies who seek to fully comply from potentially running afoul of the False Claims Act. Notably, Sec. 1655 (c) clarifies that disclosures are only to be required "if an entity becomes aware of information requiring disclosure." As proposed, however, the Rule does not tie any of the disclosure requirements to an organization's awareness of information requiring disclosure required pursuant to each subsection.

We recommend that the Rule define an appropriate, risk-based notification trigger that is based on vendors' actual rather than assumed knowledge. Similarly, the trigger for disclosures pursuant to Sec. 1655(a)(2) should be tied to actual vendor knowledge that the foreign person is, in fact, acting on behalf of a foreign government of concern. To avoid exposing contractors to unnecessary legal risk under the False Claims Act, we recommend the proposed rule be updated to require companies to provide information based on actual knowledge.

Expand OSS exemption and apply it to OSS components embedded within end products

We believe the exemption for open source software (OSS) is critical and should be strengthened. While there is no authoritative definition for OSS, we believe that the proposed definition falls short from including critical OSS use cases. For example, it is common practice to integrate OSS components into commercial and proprietary software end products. We recommend clarifying that the exemption also applies to OSS components within end products and updating the definition of OSS under Section 239.7X03. We believe a more encompassing definition would be “The prohibition at 239.7X02 does not apply to software made available to the public in source code form.”

Limit Data Access to Federal Authorities with a Need to Know

Notification mandated under the proposed rule could require vendors to provide information that is confidential business information and could, if made public, expose sensitive business strategies, proprietary product information, or other information that could potentially damage vendors.

To prevent such harm, we recommend that the implementing regulations exempt any information shared as part of a required disclosure from federal, state, and local freedom of information laws, open government laws, open meetings laws, open records laws, sunshine laws, and similar laws requiring disclosure of information or records. Further, the regulations should make it clear that information disclosed by vendors should be used strictly to improve the Department's risk management posture. The Department’s implementation requirements should limit requesting agencies’ access to the registry under Sec. 1655 (f) (2) to federal authorities (e.g., procurement officials) who have a need to know. The registry should not be available to all employees of a requesting agency. Access to the registry should be tracked, audited, and enforced. This would be in line with the principle of least privilege while also meeting legislative intent.

Strike subcontractor flow-down provisions

Section 252.239-70ZZ(g) creates sub-contractor flow-down requirements, which were not contemplated by Section 1655. Furthermore, it is unreasonable for Contractors to apply the sub-contractor requirements according with a look-back to 2013. Section 252.239-70ZZ(g)(2) requires the Contractor require its subcontractors to complete foreign obligations disclosures prior to awarding a subcontract. Considering it has been over five years since NDAA FY19 was enacted and these rules were just recently proposed, it is unreasonable to apply a look-back to 2013 pertaining to the subcontractor requirements. The disclosure of private sector contractual agreements is not a standard practice nor are requests to past or present customers for the identification of the citizenship of their personnel who may have had or currently have access to source code provided under routine business arrangements. Contractors likely have established agreements with their subcontractors and, therefore, they would automatically be in violation of Section 252.239-70ZZ(g)(2).

Strike representation and attestation requirements.

Sections 252.239-70YY(e) and 252.239-70ZZ(d)-(e) appear to introduce attestation requirements that were not contemplated under Section 1655. We note that Section 1655 does not require contractor disclosures to be input into the Government's EDA Catalog system (PIEE). Many contractors do not maintain e-catalogs in this technically optional system. Moreover, Section 252.239-70ZZ(d)-(e) could be read in tandem with the subcontractor provisions of 252.239-70ZZ(g) and the use of the term "supplier" in 252.239-70ZZ(c)(2) as creating supply chain attestation requirements, in which a Contractor would need to ensure its suppliers provide accurate disclosure. We believe these requirements exceed the scope of Section 1655 and recommend their removal from the Rule.

Define key terms

The Rule fails to define critical terms which expands the scope significantly. The Rule should provide definitions for the following terms at a minimum:

> "Code Review" We propose the following definition for your consideration: "A process wherein, in response to the direction of a foreign government, an agency of a foreign government, or an official acting on behalf of a foreign government, a vendor formally submits portions of the software code of a product, service, or system to a third party for a quality assurance review using human and/or automated methodologies. A code review is normally conducted in a laboratory or other controlled setting and may involve the use of automated static analysis or other anomaly detection tools."
>
> "Foreign government" This should be limited to governments of concern as identified by the list pursuant to Section 1654.
>
> "Foreign person" This definition should be limited to foreign persons acting on behalf of a foreign government of concern as identified by Section 1654.
>
> "Non-commercial product, system, or service" The Department should carefully define which non-commercial products, systems, or services it considers to be in scope for the disclosure requirements pursuant to Sec. 1655(a)(1). The definition should be consistent with the definition under Sec. 1655(h)(5).
>
> "Open source software" Clarify that the exemption also applies to OSS components within end products and updating the definition of OSS under Section 239.7X03. We believe a more encompassing definition would be "The prohibition at 239.7X02 does not apply to software made available to the public in source code form."

“Supplier” Section 252.239-70ZZ(c)(2) of the proposed rules uses the term “supplier” as opposed to Contractor, but the term “supplier” is undefined. The use of the term “supplier” seems to imply that the Contractor must flow-down this disclosure requirement to the subcontractors, but in section 252.239-70ZZ(g) the rules specifically reference subcontractor requirements. The proposed rules should clarify the definition for the term “supplier” in section 252.239-70ZZ(c)(2).