wiley

ALERT

DOD Seeks Contractor Disclosures of Foreign Access to Software Source Code

November 20, 2024

WHAT: The U.S. Department of Defense (DOD) issued a proposed rule to implement Section 1655(a) and (c) of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2019 (Pub. L. 115-232). The proposed rule would prohibit DOD from acquiring products, services, or systems relating to information or operational technology, cybersecurity, industrial control systems, or weapon systems if the offeror fails to provide certain disclosures related to whether the offeror has shared source code and computer code with foreign persons or governments.

WHEN: DOD published the proposed rule on November 15, 2024. Comments are due by January 14, 2025.

WHAT IT MEANS FOR INDUSTRY: The proposed rule would require offerors to affirm whether, at any time after August 12, 2013, the offeror has allowed, or is under an obligation to allow, a foreign person or government to review the code of a noncommercial product, system, or service that DOD is using or intends to use or that was developed for DOD. Offerors would also have to disclose whether they hold or have sought an export license for information technology products, components, software, or services that contain computer code custom-developed for the product, system, or service DOD is procuring. Post-award, contractors would be required to maintain these disclosures throughout the life of the contract.

The proposed rule also authorizes DOD to take action to mitigate national security risks following receipt of contractor disclosures of foreign access and may incorporate risk mitigation conditions into agreements for use, procurement, or acquisition of affected products, systems, or services.

Authors

Tracye Winfrey Howard
Partner
202.719.7452
twhoward@wiley.law

Teresita Regelbrugge
Associate
202.719.4375
rregelbrugge@wiley.law

Practice Areas

Cybersecurity

Government Contracts

Internal Investigations and False Claims Act

National Security

Strategic Competition & Supply Chain

DISCLOSURE OBLIGATIONS

The proposed rule would require offerors to make specific disclosures:

1. whether, after August 12, 2013, the entity making the disclosure has allowed a foreign person or government to review the code of a noncommercial product, system, or service that DOD is using or intends to use or that was developed for DOD;
2. whether, after August 12, 2013, as part of a sale agreement or transaction with a foreign government or foreign person acting on behalf of a foreign government, the entity making the disclosure is under an obligation to allow a foreign person or government to review the source code of a product, system, or service that DOD is using or intends to use or that was developed for DOD; and
3. whether the entity making the disclosure holds or has sought a license pursuant to the Export Administration Regulations (15 CFR chapter VII, subchapter C), the International Traffic in Arms Regulations (22 CFR chapter I, subchapter M), or successor regulations, for information technology products, components, software, or services that contain code custom-developed for the noncommercial product, system, or service DOD is procuring.

Offerors would submit disclosures within the Catalog Data Standard in the Electronic Data Access (EDA) system (https://piee.eb.mil). By submitting an offer, the contractor would be representing that the disclosures are current, accurate, and complete.

If selected for award, contractors also would have an obligation under the proposed rule to maintain these disclosures throughout contract performance and flow down the disclosure requirements to subcontractors.

KEY TAKEAWAYS

National Security Risk Mitigation. The proposed rule provides that, if the Secretary of Defense determines that a disclosure relating to a product, system, or service entails a risk to the national security infrastructure or data of the United States, or any national security system under the control of DOD, the Secretary must mitigate those risks. In addition, as the Secretary considers appropriate, the Secretary may condition any agreement for the use, procurement, or acquisition of the product, system, or service on the inclusion of enforceable conditions or requirements that would mitigate such risks.

Interest in Software Supply Chain Persists. The proposed rule is the latest in several ongoing federal efforts to gain additional insight into software supply chains and to insulate those supply chains from foreign disruption or negative influence. Many may be familiar with the secure software development attestations that federal agencies are collecting from contractors, including through a Common Form created by the Cybersecurity and Infrastructure Security Agency (CISA) that we covered here. The FAR Council also continues to develop a proposed rule about securing the software supply chain (FAR Case 2023-002).

Exceptions Are Very Limited. The prohibition and disclosure requirements would not apply to open-source software. As with other recent government cybersecurity, supply chain, and software initiatives, however, the proposed rule would apply to all procurements and contracts for products, services, or systems relating to information or operational technology, cybersecurity, industrial control systems, or weapon systems, including those for commercial products and commercial services, commercially available off-the-shelf (COTS) items, and procurements below the simplified acquisition threshold.

Scope of Disclosure. Also notable here is that the disclosures in the proposed clauses are broader than the statutory requirement. The FY2019 NDAA instructs DOD to obtain disclosures only of whether "a foreign government" has reviewed the code of a non-commercial product, system, or service developed for DOD or that DOD is using or intends to use. The proposed rule adopts a broader disclosure, however, by seeking information on whether a "foreign person or government" has reviewed such code.

Disclosure Risks. By requiring offerors to represent that information submitted on foreign disclosures is current, accurate, and complete, DOD appears poised to leverage the False Claims Act to prosecute knowing violations of the clause. The Department of Justice's Civil Cyber Fraud Initiative has been active in the past year in pursuing False Claims Act cases in which contractors' representations to the Government have not kept pace with their compliance (see here coverage by our White Collar Defense and Government Investigations team).

***

Wiley's cross-disciplinary Government Contracts and National Security practices will continue to monitor these developments.