wiley

ALERT

# FAR Council Proposes Pair of Major Cybersecurity Rules for Government Contracts

October 3, 2023

**WHAT**: The Federal Acquisition Regulatory Council (FAR Council) proposed a pair of major cybersecurity rules intended to implement key parts of President Biden's May 2021 Executive Order No. 14028 on Improving the Nation's Cybersecurity. The proposed rule in FAR Case No. 2021-0017 primarily addresses incident reporting and applies broadly to all contractors that use information and communications technology systems in the performance of a government contract. The proposed rule in FAR Case No. 2021-0019 aims to standardize security requirements for federal information systems (FIS)—the types of information systems and technology that contractors provide or maintain for the Government as a contractual obligation. Both propose significant new obligations for federal contractors.

**WHEN:** The FAR Council issued both proposed rules today with a request for comments within 60 days (Due December 4, 2023).

**WHAT DOES IT MEAN FOR INDUSTRY:** If adopted in its current form, the FAR Council's proposed rule on incident reporting (FAR Case No. 2021-0017) is likely to have the most broad reaching impact—applying across federal agencies and to all contract types, affecting approximately 75 percent of contractors, according to the FAR Council. The proposed contract clause included with the rule also would demand more from contractors than the current Department of Defense (DoD) contract clause at DFARS 252.204-7012 or the FAR clause at 52.204-21, such as "security incident" reporting to the Cybersecurity & Infrastructure Security Agency (CISA) within eight hours of discovery and every 72 hours thereafter. And, although the FAR Council frames the rule as focused on incident reporting, it includes significant requirements that apply even when a contractor

## Authors


Tracye Winfrey Howard
Partner
202.719.7452
twhoward@wiley.law

Kara M. Sacilotto
Partner
202.719.7107
ksacilotto@wiley.law

Gary S. Ward
Partner
202.719.7571
gsward@wiley.law

Teresita Regelbrugge
Associate
202.719.4375
rregelbrugge@wiley.law


## Practice Areas

Cybersecurity

Government Contracts

Privacy, Cyber & Data Governance

has not been affected by a security incident. Paragraph (c)(3) of the proposed contract clause, for example, would require all contractors to maintain and provide a current Software Bill of Materials (SBOM) "for each piece of computer software used in performance of the contract." The proposed rule also requires contractors to certify, as a condition of receiving future contracts, that they have "submitted in a current, accurate, and complete manner, all security incident reports required by" the contract clause proposed in this rule.

The proposed rule in FAR Case No. 2021-0019 is intended to standardize the requirements for FIS provided or maintained as part of a contractual requirement. Although the proposed rule focuses on defining the cybersecurity requirements that contractors must implement for these FIS, it also includes other notable obligations such as a requirement to indemnify the Government for a broad range of potential liabilities arising from both introducing unauthorized data or information into a government system or releasing information from a government system without authorization.

The Wiley team will provide further details on the key elements of both rules in a forthcoming follow-up Alert.