wiley

NEWSLETTER

What Cyber Landscape Awaits Government Contractors Following Biden's Executive Order?

July 2021

On May 12, the Biden Administration issued an Executive Order (EO) setting in motion an ambitious plan to rapidly strengthen the cybersecurity posture of the Federal government and its contractors, service providers, and software vendors. Wiley covered the nuts and bolts of the EO in a Client Alert, and did a deeper dive in a podcast last month—both are worth your time.

The cyber EO is sweeping in scope, but provides little in the way of details on what the government contracting industry can expect. Given the seemingly exponential rise in recent cyber incidents—from Solarwinds to Colonial Pipeline—the EO charts an aggressive schedule for various government stakeholders to recommend a slate of "bold changes and significant investments" the government will make in new cyber standards that will be implemented across government. Much of the heavy lifting will then be tasked to the Federal Acquisition Regulation (FAR) Council, which is charged with implementing new regulations and contract clauses to execute the EO's requirements within the government's acquisition processes. With a potential flurry of rulemaking coming, this article addresses a handful of the "known unknowns" that federal contractors should be tracking throughout the months ahead. Due to the tight timelines established in the EO, industry will likely have limited opportunities to comment and seek guidance on any proposed or interim rulemaking, and likewise will face short windows for commenting on the many inputs being developed by other federal agencies (at the U.S. Departments of Commerce and Homeland Security, among others) that will inform FAR Council's work.

Authors

Jon W. Burd
Partner
202.719.7172
jburd@wiley.law

Kara M. Sacilotto
Partner
202.719.7107
ksacilotto@wiley.law

Tracye Winfrey Howard
Partner
202.719.7452
twhoward@wiley.law

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Gary S. Ward
Partner
202.719.7571
gsward@wiley.law

Practice Areas

Cyber and Privacy Investigations, Incidents & Enforcement

Cybersecurity

Government Contracts

Privacy, Cyber & Data Governance

Requests for Equitable Adjustment, Claims, and Terminations

How broadly will the FAR define information technology (IT) and operational technology (OT) "service providers"? Section 2 of the EO focuses on removing perceived barriers to sharing threat information and increasing disclosure of information by IT and OT service providers regarding cyber threats, incidents, and risks. The disclosures are intended to improve the government's ability to identify, deter, prevent, and respond to cyber incidents. Notably, the EO calls on IT and OT service providers to collect and preserve data, information, and reporting relevant to cyber incidents involving "***all information systems*** over which they have control," which "includes"—but is not limited to—"systems operated on behalf of agencies." These IT and OT service providers will also be required to "collaborate" with Federal investigative authorities, including "by implementing technical capabilities, such as monitoring networks for threats." Given the potential broad scope of reporting and compliance, which may not be limited to just information systems used specifically in support of the government or government contracts, the scope of who qualifies as an IT or OT service provider may have profound impacts. If too broad, it may drive companies from the Federal space, or force companies with a commercial heritage, to rethink the need for separate federal subsidiaries, in order to avoid mandatory reporting to the government of incidents that do not affect government contracts or government data.

How much will new government-wide cyber standards emulate the U.S. Department of Defense's (DOD's) rules for Safeguarding Covered Defense Information? The EO notes that "[c]urrent cybersecurity requirements for unclassified system contracts are largely implemented through agency-specific policies and regulations," and "[s]tandardizing common cybersecurity contractual requirements across agencies will streamline and improve compliance for vendors and the Federal Government." The FAR Council is expected to issue new standardized contract language addressing cybersecurity requirements. This echoes DOD's efforts over the last decade to standardize cyber protection and reporting requirements in Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting. It will be noteworthy whether the FAR Council uses the existing DOD requirements (and the National Institute of Standards and Technology [NIST] SP 800-171 technical baseline) as a starting point, or creates a whole new regime. Either approach could pose challenges for industry. If the FAR Council adopts these or similar requirements modeled on DOD's current cyber regime, it would subject a broader segment of the government contracting industry to cyber requirements that have been challenging and costly for defense contractors to fully implement. On the other hand, starting anew increases the risk that any rulemaking will take the form of an evolving, iterative process, as DOD's process has been since it first issued a proposed rule in June 2011; it would also risk subjecting DOD contractors to potentially overlapping or inconsistent standards. It also begs the question of what the future holds for DOD's oft-delayed Cybersecurity Maturity Model Certification (CMMC) program, which is addressed in a companion article in this newsletter.

Will the government drive contractors to the cloud, Zero Trust Architecture, multi-factor authentication, and encryption? Section 3 of the EO prioritizes the government's "accelerate[d] movement to secure cloud services" and makes clear the government's long-term preference for centralized, standardized secure cloud technologies. It calls for the development of "a Federal cloud-security strategy" that will require agencies to adopt Zero Trust Architecture, multi-factor authentication, and encryption to the maximum extent practical. Although the EO lays out these requirements for the government, not contractors, trendlines are pushing contractors in the same direction. NIST SP 800-171 already requires DOD contractors subject to DFARS

252.204-7012 to implement multi-factor authentication for privileged accounts, and protect data at rest (albeit not necessarily through encryption); and many DOD contractors have opted to migrate activities to the cloud, rather than commit resources to harden corporate enterprise information systems to NIST SP 800-171 standards. In time, more government contractors may determine that they should do the same—either because new federal standards will require it, or because it makes better business sense.

What types of software will be subject to enhanced software supply chain requirements? Section 4 of the EO focuses on hardening the government's software supply chain, to "implement more rigorous and predictable mechanisms for ensuring that products function securely, and as intended." The EO highlights "critical software," in particular, which is being separately defined by NIST and is referred to as software that "performs functions critical to trust (such as affording or requiring elevated system privileges or direct access to networking and computing resources)." The EO identifies several standards that should be included in a more robust and controlled software supply chain, focused on ensuring the provenance of software and the integrity of development environments, including a Software Bill of Materials, vulnerability disclosure program, and vendor attestations. Although critical software is highlighted as a particular point of emphasis in the EO, the supply chain integrity objectives appear to apply broadly to all types of software that the government procures, not just critical software. Issues for industry to track include what the scope/definition of "critical software" will be, and whether any new supply chain rules will apply only to critical software, in the first instance, or to other software products. The EO also appears to limit its application to software products that the government buys directly for its own use (including sales from General Services Administration [GSA] schedule and other government-wide acquisition contracts), but does not address whether the supply chain integrity requirements will extend to software used or provided by a prime contractor—such as third-party software delivered as part of an integrated system, or deployed in a Software as a Service environment. Slight changes in the scope of applicability may generate large swings in the number and type of contractors that will be affected.

How will the government handle legacy software? For software products developed and procured prior to the implementation of the EO's new supply chain integrity standards, or for which the government is unable to obtain attestations from the vendors that the software meets the new requirements, the EO calls for agencies to "remove" those products "from all indefinite delivery indefinite quantity [IDIQ] contracts; Federal Supply Schedules; Federal Government-wide Acquisition Contracts; Blanket Purchase Agreements; and Multiple Award Contracts." Moreover, for legacy software products already deployed, agencies will have to "comply" with the new supply chain directives, or "remediate" the software. These could have sweeping impacts on (and create opportunities for) software manufacturers and vendors, as agencies may turn to them to re-engineer source code for existing products to meet the new requirements and effectively create the release of government-specific "2.0" software versions. For agencies operating legacy software products, for which the agencies likely lack access to source code—or sufficient data rights in the code—to effectively replace or "remediate" the software, contractors could find opportunities to contract with agencies both as service providers and as software vendors to assist with legacy software remediation or migration activities.

What can industry anticipate about the FAR Council's rulemakings (and their aftermath)? The EO establishes aggressive deadlines for stakeholder recommendations and rulemaking by the FAR Council. In many cases, the FAR Council is instructed to issue updated regulations and contract clauses for comment within 60 or 90 days following technical recommendations from others (including the Department of Commerce, Department of Homeland Security, Office of Management and Budget [OMB], and others). This schedule, along with the sense of urgency expressed in the EO and reflected in recent events, increases the likelihood that the FAR Council will issue interim rules for comment, and then work to refine its rules after implementing them. As we saw with DOD's implementation of DFARS 252.204-7012, this approach often led to the interim rules and new standards outpacing industry's capacity to meet them, which DOD had to accommodate by delaying effective dates and relaxing its compliance expectations.

The FAR Council may also address the flow down of any contract clauses to subcontractors, as it often does when implementing new compliance requirements. There may also be certain types of contracts or services that could be added to, or excluded from, the new rules (for example, extending application beyond IDIQ or other multiple-award type contracts), but it appears unlikely that some of the traditional FAR clause exceptions will be extended to small businesses, commercial item contractors, and/or contracts for commercial-off-the-shelf items.

Agencies will be instructed to add the new clauses to solicitations issued after the effective date. For existing contracts, contractors may see attempts by customer agencies to modify contracts unilaterally to add the new clauses, if the contract is not one for commercial items, or seek a bilateral modification for commercial item contracts. Contractors will need to be attuned to such modifications as they will likely increase the cost of performance, schedule, or both. Execution of a bilateral modification without reserving the right to seek an equitable adjustment could waive any such claim. And, to recover the increased costs, contractors will need to be tracking them carefully to enable the submission of a request for equitable adjustment or claim.

Wiley will continue to monitor developments related to the EO, including the FAR Council's rulemaking. We will update Client Alerts and deliver timely commentary through additional episodes in our podcast series.