Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Biden Order Adds Info-Sharing Onus On Wary Contractors

By **Daniel Wilson**

Law360 (May 14, 2021, 10:25 PM EDT) -- President Joe Biden's executive order aimed at protecting federal networks from cyberattacks will impose new requirements on contractors, especially those that work exclusively with civilian agencies, such as sharing information about security breaches they may otherwise want to keep confidential.

Following high-profile cyberattacks like last year's massive breach of SolarWinds Corp.'s software that compromised several federal agencies' networks, and the recent ransomware attack that locked down a major fuel supply pipeline, Biden's Wednesday order imposes a raft of new cybersecurity requirements intended to help protect federal networks against cyberattacks and better respond when they do occur.

Many of its provisions either explicitly or implicitly target federal contractors, including a clause that will strip away contractual barriers that prevent "operational technology" and information technology providers from sharing cyberthreat and incident information, data that contractors are often reluctant to disclose voluntarily. Operational technology includes systems "that run the vital machinery that ensures our safety," according to the order.

"Companies are really concerned that if they report, they may then get in trouble if it comes to light that they may not have had the proper controls in place, or they didn't do everything according to the textbook," Hogan Lovells senior associate Stacy Hadeka said.

The order is silent on potential immunity for sharing information, meaning businesses are likely to push for at least some sort of safe harbor in upcoming regulations to implement the order, Hadeka said.

But contractors may face headwinds pushing for any more than limited protections for sensitive or proprietary information, with the U.S. Department of Defense, for example, rejecting similar requests regarding an information-sharing requirement for its rule protecting controlled unclassified information, or CUI, according to Wiley Rein LLP partner Jon Burd.

"DOD was focused on having access to the information and prioritized that," he said. "I feel like the energy is similarly situated now, where the government is saying they're prioritizing having access to the information in a timely manner, and in an actionable manner. I think that's going to take priority over industry's concerns about safeguarding the information or managing the proprietary aspects of the information."

That means contractors "will have to have their cybersecurity stuff together," McCarter & English LLP government contracts practice co-chair Alex Major said.

"With the government demanding now and expecting that [information] sharing, if something goes wrong, there really isn't that, 'Well, is it, or isn't it'" consideration whether an incident should be reported, he said.

The order's requirements largely track what the DOD already expects or is pushing defense contractors toward in terms of cybersecurity and information sharing, such as through its pending Cybersecurity Maturity Model Certification program, so contractors that deal exclusively with civilian agencies are going to have the most work to do to comply.

"There's going to be a real sea change [for] civilian agency contractors," Burd said. "Until this point, they've had relatively de minimus cybersecurity obligations imposed on them through the Federal Acquisition Regulation. ... If this is going to be similar in scope and rigor [to DOD requirements], then I think this is a big moment for civilian contractors."

Other provisions of the order that will affect contractors include the formation of a Cyber Safety Review Board that will have the authority to assess "significant cyber incidents," including on contractors' networks, and a requirement to shore up the supply chain for "critical software."

And if existing software doesn't meet the new cybersecurity requirements, the order directs agencies to pull related products from all federal indefinite-delivery, indefinite-quantity contracts, which includes tens of billions of dollars of governmentwide acquisition contracts like the General Services Administration's Federal Supply Schedule.

"I see that as kind of a big issue not just for software manufacturers, but also for software resellers, distributors and system integrators," Major said. "That is a significant piece of the executive order."

One positive aspect of the order for contractors is that it also calls for cybersecurity requirements to be uniform across the government, in place of the current piecemeal approach among agencies.

"Industry has really been pushing for that for a long time," Hadeka said. "I've had experiences with clients where each agency has their own unique cybersecurity requirements, such as one-hour [incident] reporting, also even down to the data location. It's really onerous for contractors to try to figure all that out and understand what their full obligations are."

Another potential benefit for contractors is the order's call to modernize the Federal Risk and Authorization Management Program, or FedRAMP. Intended to standardize security requirements for cloud service providers, its implementation has been inconsistent across different agencies.

"Modernization of FedRAMP is both necessary and essential, given how important FedRAMP is as a regulatory program," Crowell & Moring LLP privacy and cybersecurity group co-chair Evan Wolff said.

The full scope of the order's impact will depend on how it's implemented through regulation, with specific definitions of some key terms, such as what counts as "critical software," and what products should be on a list of critical software, being left to agencies to decide.

The order gives only a broad definition of "software that performs functions critical to trust (such as

affording or requiring elevated system privileges or direct access to networking and computing resources)."

"The way that definition is written in the executive order could include just about any piece of software that the government uses, including commercial-off-the-shelf software that is ubiquitous, such as a word-processing program or a spreadsheet program," Holland & Knight LLP partner Eric Crusius said.

The definition of "information and communications technology" service providers that will be required to "promptly report" cyber incidents involving a software product or service is also up in the air, and if defined broadly could include most services contractors, which often provide IT services as part of their work, according to Crusius.

"You're going to bring in a lot of contractors that don't have really any clue that they're going to have to comply with a new regulatory regime," he said.

The order includes an aggressive timeline for implementation, with agencies given deadlines of between 45 and 120 days to start implementing many of its key requirements for contractors, meaning the rulemaking process should start this summer with initial proposed or interim rules.

Crusius recommended that contractors be engaged in the rulemaking process to "help shape the policy in a way that will bring about regulations that are effective, but also not overly burdensome for them."

But final implementation could be years away, with dozens of requirements to codify into regulation. The DOD's iterative process for its CUI rule, for example, took several years to be finalized, and as the agency's ongoing CMMC implementation process also shows, "not everything works the way they think it will — it takes time," Hadeka said. "There's trial and error."

Another wrinkle that could also drag out implementation is the order's requirement to remediate legacy government systems and software products that don't meet the new cybersecurity standards.

The government uses thousands of legacy software products, according to Burd, and it will be a herculean task to fix or replace those that aren't up to par, especially because in many cases contractors likely don't have the data rights needed to make necessary changes to source code, if they have access to the source code at all.

"I think that is a potential sleeping giant in this EO that could create long-term opportunities, but it also is going to have long-term repercussions," he said.

--Editing by Breda Lund and Emily Kokoll.