wiley

MEDIA MENTION

Jon Burd Discusses President Biden's Cybersecurity Executive Order

Law360
May 18, 2021

Jon W. Burd, partner in Wiley's Government Contracts, National Security, and Privacy, Cyber & Data Governance practices, was quoted in a May 14 *Law360* article about President Biden's recent Executive Order (EO) on Improving the Nation's Cybersecurity.

As reported in the article, many of the EO's provisions target federal contractors, including a clause that would remove contractual barriers to sharing information about cyber threats and incidents. Mr. Burd co-authored a Wiley alert on the EO on May 13.

As regulations are developed to implement the EO's information-sharing provisions, contractors may face resistance in seeking exceptions beyond just limited protections for sensitive or proprietary information, Mr. Burd said. He noted that the U.S. Department of Defense (DOD), for example, rejected similar requests for exemptions to an information-sharing requirement for its rule protecting controlled unclassified information.

"DOD was focused on having access to the information and prioritized that," Mr. Burd told *Law360*. "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."

The EO also signals "a real sea change" for civilian agency contractors, according to Mr. Burd. "Until this point, they've had relatively *de minimus* cybersecurity obligations imposed on them

Related Professionals

Jon W. Burd
Partner
202.719.7172
jburd@wiley.law

Practice Areas

Government Contracts
National Security
Privacy, Cyber & Data Governance

through the Federal Acquisition Regulation," he said. "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."

The EO also requires federal agencies to remediate legacy software that does not meet the new cybersecurity standards. Noting that the government uses thousands of legacy software products, Mr. Burd said it will be an immense task to fix or replace those that are not in compliance – in part because the government likely doesn't have access to source code, or sufficient data rights in software, to make necessary changes to source code.

"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," Mr. Burd said.

To read the article, click here (*subscription required*).