Bloomberg BNA

Federal Contracts Report™

DOD

Interim Rule on Reporting Cyber Breaches Burdensome for Contractors, Analysts Say

The Defense Department's Aug. 26 interim rule directing contractors to report cybersecurity breaches greatly expands the types of information that must be protected.

Previously, contractors had to protect unclassified controlled technical information. They now must protect ''critical information'' that concerns ''operational security,'' information subject to export controls, and ''any other information'' that requires safeguarding or dissemination controls, Rogers Joseph O'Donnell Shareholder Robert Metzger told Bloomberg BNA Aug. 26.

These categories are so broad that they could include proprietary information or information used in support of contingency operations, and contractors will find it hard to argue that particular types of data are beyond the rule's reach, according to Dentons Senior Managing Associate Michael McGuinn.

Contractors also will grapple with the impact on their supply chains because requirements flow down to subcontractors and cover small businesses. Firms had hoped for a small business exemption, but the rule writers declined to provide one.

Metzger said the DOD's estimate that the rule will affect about 10,000 contractors might be low, in part because the requirements apply to common commercial item purchases.

The rule implements provisions in the fiscal 2013 and 2015 National Defense Authorization Acts requiring contractors to report cybersecurity incidents. It also implements policies on purchasing cloud computing services.

Benefits for Contractors. The interim rule has some benefits for contractors, Reed Smith LLP Partner Larry Block told Bloomberg BNA Aug. 25.

For example, it protects from public disclosure the proprietary information that contractors might have to share with the federal government following a cybersecurity incident.

However, the rule is unclear about just how the government must protect this information—an issue that should be addressed in the final rule, Block said.

The rule also clarifies that reporting an incident, in and of itself, isn't evidence of an inadequate security system, Block said. An inadequate security system could be the basis for finding a contractor has an inadequate business system and is therefore ineligible for new contracts.

Keep Track of Compliance. Several provisions of the interim rule might cause problems for contractors that don't carefully monitor compliance, Sheppard Mullin Associate Alexander Major told Bloomberg BNA Aug. 26.

For example, the rule requires contractors to notify the DOD if they will use cloud computing services, Major said. A contractor might not need cloud computing at the start of a contract but might later on, so communication between contract and IT personnel is important, he said.

In addition, the rule requires contractors to protect specific data for a contract using the security requirements found in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, or to get approval from the DOD's chief information officer to use other requirements.

However, contractors might use data interchangeably on different contracts, Major said. For example, they might have pre-existing data covered under a prior standard such as NIST SP 800-53, but if they experience a cyber attack, the federal government might hold them to the standards found in NIST SP 800-171.

NIST SP 800-171 standards are slightly broader than NIST SP 800-53 standards, which applied under previous Defense Federal Acquisition Regulation Supplement clauses, Major said. Contractors should make sure they know which standards apply to their data and should consider using NIST SP 800-171 as described in the interim rule.

Cloud Computing. The rule states that a cloud computing provider must keep servers handling covered information in the U.S., Mintz Levin Member Jonathan Cain told Bloomberg BNA Aug. 25. Many contractors keep them in other countries and will need to set up servers separately just for defense work, which might be costly.

This requirement flows down to subcontractors, although they might not know it. That means subcontractors could inadvertently use an unapproved cloud service for a prime contractor's data, he said.

Better Definitions. A few definitions in the rule should be clarified, Carl Herberger, a vice president of IT security provider Radware, told Bloomberg BNA Aug. 25.

For example, the rule directs contractors to store 90 days of routine data but doesn't specify whether it's transactional data, encrypted data, or all data.

It also doesn't define what constitutes a data breach. To a lay person, a cyber incident could be a mishap in-

volving a user ID password combination, Herberger said.

''Where you have gray areas in security, you have shadows,'' he said. ''And in shadows you have murkiness, and in murkiness you have noncompliance.''

The interim rule is available at: https://www.federalregister.gov/articles/2015/08/26/2015-20870/defense-federal-acquisition-regulation-supplement-network-penetration-reporting-and-contracting-for

By David Hansen

To contact the reporter on this story: David Hansen in Washington at dhansen1@bna.com

To contact the editor responsible for this story: Jeff Kinney at jeffkinney@bna.com

  FCR ISSN 0014-9063