Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Waiting On Cybersecurity Laws, Agencies Toughen Regs

By **Dietrich Knauth**

Law360, New York (March 26, 2012, 9:16 PM ET) -- Government contractors will continue to face inconsistencies in federal agencies' efforts to tighten and toughen cybersecurity standards through their existing legal authority, as Congress mulls competing proposals for far-reaching cyber legislation, attorneys say.

Some agencies, like the U.S. Department of Defense, General Services Administration and Department of Veterans Affairs, have moved more proactively on cybersecurity than others, with some addressing the issue through regulations and others seeking to police cybersecurity through contracts terms.

“There are surprisingly few uniform standards of care for cybersecurity requirements that apply to all government contracts,” Jennifer Zucker of Wiley Rein LLP said. “What you tend to see right now is kind of a patchwork of different requirements.”

Many of the security requirements are incorporated by reference to guidelines or standards published elsewhere, such as an agency's internal policy documents or by the National Institute of Standards and Technology. Forcing contractors to search and cross-reference the disparate standards is expensive for contractors, and increases the risk of noncompliance through omission, attorneys say.

"Somebody's going to sit down and read all of the regulations and references," David Bodenheimer of Crowell & Moring LLP said. "The lack of uniformity is one of the things that drives [contractors] nuts."

An agency by agency approach could lead to more regulation and more burden on contractors because each agency could attempt to use previous regulations as a baseline from which to add new requirements. While having more security standards will increase contractor costs, Bodenheimer said it doesn't necessarily lead to better security.

“Security is generally a ratchet effect,” Bodenheimer said. “It never becomes less, it always becomes more.”

The DOD has taken a lead role in cybersecurity after investing in shoring up its own security systems for critical and classified information, and now is requiring its contractors to follow suit.

"DOD's perspective is that their weakest link right now is their contractors," Zucker said.

In June, the department published a notice of advanced rulemaking saying that it intended to issue new regulations to improve the security of nonclassified information stored and managed by contractors.

Information that the DOD designated as critical program information, subject to export controls, exempt from mandatory public disclosure, bearing a designation of controlled access and dissemination, or personally identifiable, would be subject to new controls intended to safeguard that information from unauthorized access, and contractors would be required to notify the agency of any breaches, the notice said.

The DOD has not yet issued a rule based on that notice, but appears to be taking industry concerns seriously in is formulation of the regulation.

“I think there was a lot of concern from industry in terms of how they were going to implement the regulation and that it be done in a practical manner,” Zucker said.

The GSA, which often buys information technology services on behalf of other government agencies, has also been proactive in addressing cybersecurity concerns. The GSA has issued a number of specific requirements, such as demanding the ability to audit and inspect security systems — a tactic that Bodenheimer says is counterproductive because more access leads to more opportunities for mistakes and security leaks.

“Every audit and every penetration introduces a new vulnerability into the system,” he said.

The VA, which was recently burned by lax data security when a contractor lost computer tapes holding medical records of 4.9 million beneficiaries of the military's health insurance program Tricare, has also been active in cybersecurity. Zucker said she has seen VA contracts that include putting monetary penalties for the loss of personally identifiable information in its contracts — 37 cents per record lost.

Science Applications International Corp. which has provided support services under Pentagon contracts for more than two decades, was obligated to pay any costs associated with a data breach resulting from the Sept. 13 theft of computer tapes from an employee's car. SAIC also agreed to provide credit monitoring for all of the beneficiaries whose data was lost, and cover the costs of notifying the beneficiaries about the stolen data.

After the loss of the tapes, which contained names, addresses, lab test information, diagnoses, treatment information, provider names and locations, and other personal data, SAIC and Tricare were hit by four class actions related to the breach.

The U.S. Securities and Exchange Commission has also issued a nonbinding guidance requiring companies to disclose cyber risks if they are "among the most significant factors that make an investment in the company speculative or risky." The SEC said that companies should consider the severity and frequency of prior cyber incidents, probability and likely magnitude of future events, and the adequacy of efforts to prevent future attacks.

While there is a broad consensus among legislators and experts that new legislation is needed to address broader weaknesses in U.S. cybersecurity policy — such as the need to protect critical infrastructure and to share information about emerging threats — lawmakers may not be able to reach a workable compromise during a tense election season. In the meantime, agencies are continuing to issue regulations to supplement security guidance created under the Federal Information Security Management Act, or FISMA.

“We've been waiting for cybersecurity legislation since 2008,” Bodenheimer said. “The regulations are here and now.”

Under FISMA, the Office of Management and Budget and NIST take the lead in setting minimum security requirements, such as giving tips for secure passwords, or requiring physical security for sensitive computer systems.

Those broad, governmentwide requirements somewhat mitigate the threat of inconsistent agency regulations, according to McKenna Long & Aldridge LLP partner Elizabeth Ferrell.

“It may be piecemeal, it may be different from agency to agency, but the basic standards are going to be the same,” Ferrell said.

--Editing by Andrew Park.