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

Finally, Cyber Help For Small Businesses Is On Its Way

By **Evan Wolff, Paul Rosen, Kate Growley and Michael Gruden** (October 1, 2018, 2:23 PM EDT)

Evan Wolff

Paul Rosen

Kate Growley

Michael Gruden

The government has recognized that small- and mid-sized contractors can be the weakest link when it comes to safeguarding information. This aligns with sentiment from the small business supply chain that government cybersecurity standards can be burdensome for contractors lacking the infrastructure and resources that major defense contractors employ. The government has responded to this dilemma through recently passed cybersecurity legislation that aims to help smaller government contractors in their efforts to safeguard sensitive customer data.

The NIST Small Business Cybersecurity Act requires the National Institute of Standards and Technology to issue guidance and resources, within the next year, to help small- and medium-sized businesses identify, assess and reduce cybersecurity risks. Under the act, NIST must also:

- Ensure future resources can vary with the nature and size of the small business, as well as the nature and sensitivity of the data handled;
- Encourage the use of technology neutral, commercial off-the-shelf solutions; and
- Promote awareness of basic controls, a workplace cybersecurity culture and third-party stakeholder relationships.

Part of a Broader Effort

Partly in response to the rising number of cyberattacks targeting small businesses, the legislation is the latest in a series of efforts more broadly focused on supply chain security throughout the procurement process. Earlier this year, H.R. 5515, the John S. McCain National Defense Authorization Act for Fiscal Year 2019 was signed into law. The FY 2019 NDAA includes a robust set of cybersecurity provisions impacting the defense industrial base. Specific to small businesses, Section 1644 encourages the U.S. Department of Defense and NIST to assist small businesses in the defense industrial supply chain by:

- Enhancing awareness of and training on cybersecurity threats;
- Conducting outreach events to help small manufacturers improve their cybersecurity;

- Helping small businesses conduct voluntary cybersecurity self-assessments; and
- Ensuring small businesses understand operating environments, cybersecurity requirements, and existing vulnerabilities through mentor-protégé programs, small business programs, and engagements with defense laboratories and test ranges.

Section 1644 also authorizes the establishment of the Cybersecurity for Defense Industrial Base Manufacturing Activity, tasked with assessing and strengthening the cybersecurity resiliency of the DIB. Specifically, the Cybersecurity Activity is responsible for disseminating cybersecurity resources, assisting vendors with voluntary cybersecurity self-assessments, and promoting the transfer of DOD technology and cybersecurity techniques to small manufacturers and universities.

These recent legislative efforts focused on enhancing cybersecurity resources for small businesses build upon others made by the government to strengthen supply chain safeguarding. Last year, NIST released the NIST Manufacturing Extension Partnership Self-Assessment Handbook. The purpose of the handbook is to assist small. manufacturers protect covered defense information, a form of unclassified but nevertheless sensitive DOD information provided to contractors that comes with strict cybersecurity requirements under the Defense Federal Acquisition Regulation Supplement Clause 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting." Those requirements include ensuring adequate security for CDI by implementing the cybersecurity standard NIST Special Publication 800-171, which includes more than 100 unique technical, physical and administrative controls.

But What's Being Done Now?

While resources offered by the government continue to develop, small- and medium-sized businesses are turning to alternative strategies to lessen the challenge that traditional cybersecurity standards like NIST SP 800-171 can pose.

For some, help can be found in the use of managed service providers. These third parties can alleviate the infrastructure constraints and financial resources that are often cited by small businesses as a barrier to meeting many NIST controls. MSPs can provide an integrated solution that can be increasingly cost effective for small businesses since MSPs are acquiring and managing the requisite technical solutions that are often too costly for small business on the cusp of entering the federal cybersecurity arena. Instead, MSPs can absorb the costs associated with many of the NIST controls and spread them across their client base. The result can be a significant reduction in upfront investment of financial and operational resources for small businesses seeking to meet NIST cybersecurity standards.

Another product that small businesses are contemplating as they devise their internal cybersecurity plan is insurance. Cyber insurance can encompass third-party losses (liability to others), as well as first-party losses (losses to the policyholder's own business interests). Cyber coverage programs are often negotiated based on individual company needs, which can make this offering more affordable for small businesses. But because cyber insurance is a relatively new type of policy, forms are not yet standardized. As a result, various insurers' and brokers' policy forms can differ in the scope of coverage provided. Small businesses thus tend to determine what scope of coverage meets their operational needs and the risk portfolio they're willing to accept. Types of losses that cyber insurance may cover include, among others:

- Privacy and network security risk and liability;
- Privacy regulatory fines and penalties;
- Dependent business interruption/dependent system failure;
- Cyber extortion;

- Digital assetrestoration;
- Breach event expenses; and
- Network business interruption.

Small businesses are also strategically considering the cybersecurity risks they assume through prime contractor and vendor relationships. In the defense supply chain, some small businesses are alleviating their otherwise heightened safeguarding requirements by refusing the exchange of covered defense information. That is, CDI is sometimes being transmitted down the supply chain, even though the sensitive data is not integral to performance under those contracts. Even where CDI is integral, small businesses can reduce the burden of safeguarding sensitive data if they coordinate alternate means of accessing CDI from the sender. For example, small businesses can obtain alternate access to CDI through a prime contractor's secure portal or by visiting a prime contractor's facility. They can also accept the CDI in hard copy and never carry electronic copies on their network. Not only can reducing the unnecessary transmission of CDI be a beneficial data minimization practice, but it can also reduce incumbent financial obligations and cybersecurity responsibilities.

Small businesses are a fundamental component of today's supply chain. Many provide unique and otherwise unavailable resources for some of the government's most pressing procurement needs. The industry is cheering the government's push to identify better tools to help secure small business networks. But in the meantime, the supply chain is working creatively to come up with some options of its own.

Evan D. Wolff is a partner at Crowell & Moring LLP and co-chairs the firm's privacy and cybersecurity group.

Paul M. Rosen is a partner at the firm, a former federal prosecutor and former chief of staff at the U.S. Department of Homeland Security.

Kate M. Growley is a counsel at the firm.

Michael G. Gruden is an associate at the firm.