AVIATION WEEK
NETWORK

Executive Roundtable for the Aerospace Supply Chain

The Clock is Ticking on Supply Chain Cybersecurity

October 24, 2017
Co-located with
SpeedNews' 3rd Annual AerospaceDefenseChain Conference
The Ritz-Carlton Tysons Corner • McLean, VA
By: Tam Harbert; edited by Michael Bruno, Aviation Week Network

Sponsored by

EXOSTAR®

Produced by
SpeedNews
CONFERENCES

Aviation Week Executive Roundtable

The Clock is Ticking on Supply Chain Cybersecurity

As leaks of sensitive information by defense contractors make headlines, the security of the defense industry supply chain is becoming an increasingly hot topic. In May 2017, sensitive files of a large contractor were found on a publicly-accessible Amazon cloud. In October, Australian officials said a hacker stole non-classified information on several defense programs by breaching the network of a defense contractor.

Now, starting Jan. 1, 2018, U.S. defense prime contractors and their suppliers will be held accountable for the security of their systems. A new regulation, Defense Federal Acquisitions Regulations Supplement (DFARS) 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, will require “covered defense information (CDI)” that is generated, stored or transmitted through a contractor’s system to meet 110 security requirements described in National Institute of Standards and Technology (NIST) Special Publication 800-171. Primes are required to flow these requirements down their supply chain. They are also required to report cyber incidents to the Defense Department within 72 hours, and to preserve and provide related information and documentation of the incident.

The regulation is an effort to increase security across the entire supply chain of any given contract. Yet, there are many questions, and a lack of clear definitions, which have suppliers – particularly those in the second and third tiers – struggling. Notably, those tiers may be where the greatest dangers lie. Prime contractors are tough targets for hackers because they have the money and the specialized staff to lock down systems. So hackers are moving to contractors’ supply chains – where primes spend two-thirds of their product and service costs – which are made up of thousands of companies that may be vulnerable.

More than 40 executive-level representatives from primes to Tier 2 and consultants participated in an October 24th Roundtable on these topics. The roundtable was conducted under Chatham House Rules. Accordingly, this paper summarizes the discussion, with no identification of attendees.

Participants in the roundtable broke into five groups to discuss how companies can comply with the new regulation. Among the questions pondered:

- What is the most meaningful guidance that the Pentagon, prime contractors and higher tier subcontractors can provide to small businesses to help them reduce cybersecurity risks and meet the requirements?
- How will companies identify CDI to their subcontractors? How are companies expecting CDI to be identified by their customers, partners and suppliers?
- What one thing about the cyber DFARS regulations would they change to make them more effective?

The biggest problem that companies are struggling with is a lack of clarity on CDI. There are neither definitions nor guidance on what constitutes CDI. “That’s really the elephant in the room here,” said one participant. Many wanted the government to specify exactly what CDI is, to set up various categories or classes of CDI, and to rank them in terms of priority. For example, some information might be considered the crown jewels and would get the highest level of protection, while other information would require less stringent measures. Several groups suggested that the government, or the prime contractor, identify what it considers to be CDI in every contract. Otherwise each company may operate based on its own definitions and priorities.

“For the regulations to be effective, the government really needs to say what’s most important,” said a representative of a large prime. “That’s been one of the biggest things we and our peers are pushing. We’re asking them to avoid boiling the ocean here.”

Another big problem discussed was the difficulty of small and midsized companies to meet the requirements due to resourcing. Several people noted that they don’t even know where to go with their questions. The Defense Department should clarify who is the contact so companies can ask for guidance. Even large contractors are dealing with a different person in each of the services.

Participants also emphasized the cost of compliance, a particular burden for small suppliers. One group suggested government designate approved security vendors, perhaps with special pricing, where small suppliers can go for help. One attendee noted that one of her company’s suppliers tried to use NIST’s Manufacturing Extension Partnerships but found only one vendor in the supplier’s region, and it was expensive.

“They were told it would cost $60,000,” the participant said. “And since there was only one company listed, the supplier couldn’t shop around.”

Attendees discussed using incentives to aid suppliers. Prime contractors could offer monetary rebates to suppliers that best met the requirements, for example.

Participants also discussed how or whether suppliers could avoid the new regulations. One group suggested contractors be more selective in what information they share. Although it’s mandatory to flow down the requirements, it’s not mandatory to flow down so much sensitive information. Indeed, a representative of a large prime contractor admitted that “sometimes we give a supplier a whole chapter when all it really needs is one paragraph.”

Others suggested reverting to “stone-age solutions,” i.e. sharing information non-electronically. Print information on paper, for example, and mail it via FedEx. The recipient could then lock that paper into a physical safe. Under such a scheme, could suppliers “self-delete” clauses in their contracts that govern sending and storing CDI electronically? This remained an open question.

Some primes are helping their suppliers by providing training and best practices on how to comply with the new provisions. After all, it’s in the primes’ interest to minimize disruption to their supply chains. In some cases, a small supplier may be the sole source of critical technology.

Still, small suppliers may need more assistance than a prime can provide. One participant said his company outsourced compliance to a third-party expert.

A couple of groups suggested that certification similar to the ISO certifications for quality management would help. Companies would have to regularly re-certify, so such a program would ensure consistency regardless of changes at a company, such as a corporate reorganization.

The challenges in meeting the requirements of DFARS 252.204-7012 are best met by teaming with partners, even with competitors. The representative of a large prime cited the example of the Defense Security Information Exchange (DSIE). “Collaboration is a force multiplier,” he said.

Participants agreed that the emphasis should be on keeping information secure, not just complying with the regulations. In a world of advanced persistent threats and nation-state cyber espionage, both industry and government know their leaks could endanger national security. One group noted that while the new requirements apply to electronic information, there are often leaks of information the old-fashioned way – through human beings. Training people in how to (and how not to) handle sensitive information is needed to lessen that type of security risk. It was also noted that the protection of the supply chain is a not a one-time deal, but rather a never-ending process. Companies need to identify where the data is, assess how it's being protected, mitigate the risks, validate and then start again.

Conclusion

DFARS 252.204-7012 is designed to protect sensitive information that could potentially impact national security. The participants in this discussion appreciate the importance of keeping this data secure. However, they have concerns and questions about the practical details of implementing the controls. Primes may be able to provide some help, as might third-party experts and solution vendors, as a Dec. 31, 2017, compliance deadline looms. But all involved must see the push for cybersecurity as a long-term effort that continues, just as cyber threats endure. The clock is ticking.

Participating organizations

A Company of One, Alderman & Company, Austal USA, Aviation Week Network, BAE Systems, Composite Resources, Department of National Defence (Canada), Exostar, Fairmont Consulting Group, Honeywell Aerospace, IBM Global Business Services, It's Just Results, Ivion Group – Aerospace Consulting, Kellstrom Defense, Liebherr-Aerospace Saline, Lockheed Martin, Moog, Netwatcher, Northrop Grumman, Parker Aerospace, SAIC, Schaeffler Group, Senior SSP, Sunshine Metals – A Member of AMA, Supply Dynamics, Swift Engineering, Valuepoint Group, Verify

History and purpose of the Roundtable

The Roundtable was conceived to bring together executives from various aerospace and defense manufacturing segments to cooperate through brainstorm-style discussion of ways to improve overall industry performance and execution. Previous roundtables have covered a wide variety of topics since they were initiated in 2004. Participants engage with each other on the selected topic to resolve some of the issues posed and identify their best recommendations for near-term solutions—defining near-term as about 18 months. So-called Chatham House Rules is observed, keeping comments of participants anonymous to encourage an honest discussion of both the issues and solutions.

The October 24 roundtable was hosted by Michael Bruno, Aviation Week Business Editor, Co-hosted by Jim Connelly, Lockheed Martin and sponsored by Exostar.

Exostar

Exostar offers cloud-based solutions to help companies in highly-regulated industries mitigate risk and solve identity and access challenges. Organizations leverage Exostar solutions to help them collaborate securely, efficiently, and compliantly with their partners and suppliers. Exostar provides connect-once, collect-once, certify-once access to partners. This strengthens security, reduces expenditures, and raises productivity so organizations can better meet contractual, regulatory, and time-to-market objectives. Founded in 2000 and headquartered in Herndon, VA, Exostar's solutions are used by over 135,000 organizations in over 150 countries worldwide. Exostar's A&D customers include global market leaders such as BAE Systems, Boeing, CSC, Honeywell, Huntington Ingalls Industries, Lockheed Martin, Northrop Grumman, Raytheon, and Rolls-Royce. For more information, visit www.exostar.com