United States Senate Committee on Armed Services

Subcommittee on Cybersecurity

March 26, 2019

John Luddy
Vice President, National Security Policy
Aerospace Industries Association

Chairman Rounds, Ranking Member Manchin, and Members of the Subcommittee:

Thank you for your efforts to highlight the importance of a secure supply chain and for inviting me to contribute to today's discussion. The Aerospace Industries Association (AIA) represents nearly 340 manufacturers, suppliers, and service providers across every sector and tier of the aerospace and defense industry; our 2.4 million people are the backbone of the American economy, and crucial partners in protecting our national security.

Our industry is fully committed to partnering with the U.S. government to stay ahead of cyber threats and ensure resilience throughout our industrial base. AIA has just issued a report called "What's Next for Aerospace and Defense: A Vision for 2050." The report paints a picture of the technologies and innovations that experts in our industry believe will be driving the way we move, connect, explore, and defend our interests thirty years from now. The future we envision is exciting – and it depends entirely on robust and reliable cybersecurity. So we share concerns raised by senior Department of Defense leaders about the cybersecurity of U.S. military systems, and of our entire acquisition process.

I also want to emphasize that we at AIA are pleased with the level and quality of dialogue we are having with DOD on cybersecurity and other matters. Cybersecurity is a prominent topic at quarterly meetings of our CEOs with Under Secretary of Defense for

Acquisition and Sustainment, Ellen Lord and her senior staff. I also convene quarterly engagements with Vice Admiral David Lewis, Director of the Defense Contract Management Agency (DCMA), and other DOD officials; we held the fourth of these meetings last week and have now institutionalized them as a forum to iron out the specifics of cybersecurity policy and implementation.

This afternoon, I will focus on three areas: first, on the way DOD defines the information that contractors must protect; second, on the need for cybersecurity policy to be clear, consistent, adaptive, and scalable – both across DOD and with industry; and finally, I'll highlight AIA's National Aerospace Standard 9933, "Critical Security Controls for Effective Capability in Cyber Defense," which we are now working to improve and bring into wider industry use in collaboration with DOD.

Defining What Needs To Be Protected

My first point is fundamental: the initial step in gauging appropriate cybersecurity is understanding what information needs to be secured. Obviously, classified information is clearly marked, and handled through separate and secure channels. But DOD and industry also handle an enormous amount of Controlled Unclassified Information, or CUI, some of which is further designated as Covered Defense Information, or CDI. This CDI is the focus of our ongoing shared cybersecurity efforts.

In August 2015, DOD implemented Defense Federal Acquisition Regulation Supplement (DFARS) cybersecurity clause 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting." This clause defines CDI as:

> *"…unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry, as maintained by the National Archives and Records Administration, that requires safeguarding or*

dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is—

(1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DOD in support of the performance of the contract; or

(2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

With this rule, DOD significantly increased the range of information that could be defined as CDI – and thus needing protection – to nearly everything that a major defense contractor uses to perform contracts for DOD. As a result, as specific DOD customers – the Army or Air Force, for example – determine and identify which unclassified information must be protected on contractor networks and in communications between the DOD and the industry supply chain, there has been a tendency to over-protect mundane or basic information with complicated marking requirements – there are over 100 categories of CUI in the National Archives Records and Administration (NARA) CUI Registry, and the guide to marking CUI is 41 pages long. DOD and industry must work cooperatively to identify the unclassified information that is truly important to our national security interests. The current definition of CDI must be refined so that our limited resources can be applied to the most sensitive elements of our unclassified information. If we drive resources to protect everything currently considered CDI, we will protect nothing.

Clear DOD Policy

My second concern stems from the absence of a unified DOD approach to cybersecurity policy, which has led to different customers within DOD adding requirements beyond the Defense Federal Acquisition Supplement (DFARS) requirement for contract compliance, the National Institute for Standards and Technology (NIST) Special Publication 800-171, "Protecting Controlled Unclassified Information in Nonfederal

Systems and Organizations." This too often occurs without any engagement with industry regarding the feasibility and costs associated with enhanced, agency-specific measures. This lack of uniformity complicates the landscape and adds significant ambiguity as companies are expected to comply with a burgeoning list of Service-unique requirements, resulting in segmented infrastructure, limited visibility and duplication of resources within contractor networks. Further, industry strongly believes that the customary regulatory process should be followed for these new requirements, with industry feedback leading to a more coordinated and informed rule, instead of the ad hoc, Service-by-Service approach that is occurring now.

It is not practical, affordable or safe for the government and industry to implement Service-by-Service cybersecurity requirements and evaluation criteria because our adversaries will exploit the gaps this creates. We must have a unified approach to apply mass and strength to our solutions. Recently, to align the efforts of several DOD organizations, Under Secretary Lord issued two memos directing Vice Admiral Lewis to perform specific actions for contracts overseen by DCMA. We commend Ms. Lord for her efforts to bring clarity and urgency to DOD cybersecurity efforts. Her memoranda raise complex and important legal and policy issues, however, and it is essential that these be carefully and collaboratively assessed if we are to promote our shared objective of enhanced cybersecurity for DOD programs and the Defense Industrial Base. Accordingly, we have asked to engage with her staff to discuss ways to effectively and efficiently achieve these goals.

National Aerospace Standard 9933

I will close by discussing AIA's most recent, tangible response to the cybersecurity challenge. In an effort to advance industry's partnership with the DOD, late last year AIA released National Aerospace Standard 9933, "Critical Security Controls for Effective

Capability in Cyber Defense," to provide a better way for our companies to assess their vulnerability to the dynamic cyber threats they face daily. It was developed to address two realities facing our industry.

First, while we support having standards and reporting breaches, we have maintained that the DOD's implementation of NIST SP 800-171 constitutes a static solution to a dynamic problem. Adversaries are constantly evolving their tactics and consequently there are no silver bullets and/or one-time solutions that will address the challenges we face. Second, the dynamic nature of cyber security today makes it extremely difficult for small to mid-size suppliers to create self-sustaining cyber security programs capable of managing the risk posed by advanced adversaries.

There is strong precedent for using this standards-based approach. AIA's National Aerospace Standards (NAS) program began in 1941. Standards reduce cost, increase safety, provide commonality, are recognized throughout industry, and are used by private, public, corporate, and government entities. National Aerospace Standards are voluntary and developed through a consensus-based process by the aerospace industry. Subject matter experts from AIA member companies participate in committees and working groups to develop and maintain the NAS library, which currently contains over 1400 active standards.

To set a viable cybersecurity baseline for the aerospace and defense industry, AIA developed NAS9933, which is built upon the Exostar Cyber Security Questionnaire and information published by the Center for Internet Security (CIS).[1] The standard contains five capability levels. Instead of a one-size-fits-all checklist for compliance, this format

[1] Exostar is a cloud-platform company initially founded via a partnership with the major defense prime contractors and offers cloud-based secure business collaboration solutions.

establishes Capability Level 3 as a minimum performance level, with Levels 4 and 5 as higher-level objectives.

To illustrate: a company that achieves Capability Level 3 has a solid performing cybersecurity risk management program and strong technical network protections in place to protect critical information, which make it harder for an adversary to penetrate the company's systems; the company has demonstrated they understand the nature of advanced threats and are taking steps to address these threats. At Level 4, a company can detect, protect against, and respond to advanced threats – for example, by using virtual machines and air-gapped systems to isolate and run applications; a company at Level 5 has optimized network protection based on the changing nature of the threat – for example, by requiring multi-factor authentication for accounts that have access to sensitive data or systems.

We intend for NAS9933 to establish the cybersecurity baseline in the aerospace and defense industry, and to support government leaders' efforts to align with industry and move beyond minimal compliance toward greater risk- or threat-based security. As with all standards, there is always room for improvement. We view NAS9933 as just a starting point and look forward to developing it further to best aid our industry partners.

To be clear, our standard is designed to serve as a maturity model of best practices for helping companies improve their cybersecurity programs. It is not intended to replace or supersede the government's mandated controls, nor should it be used as an evaluation tool to score companies and assign ratings. As I have stated, enduring DOD and industry partnerships need to be established and leveraged to continually evolve our collective approach to this problem. The DOD and industry bring unique

perspectives, experiences and equities to the table to address these challenges – only by working together will we be successful.

We have reason to believe that the Department of Defense supports our approach. Since we published NAS9933 last fall, several DOD leaders have praised the work and have begun to work with us to use it as the baseline for an enhanced standard for both industry and DOD cybersecurity activity. We welcome this next step and look forward to working together to improve protections across the cybersecurity domain.

AIA recognizes the national and economic security threats from cybersecurity vulnerabilities and shares DOD's commitment to strengthening our cyber defenses. This issue is simply too important to be handled in a piecemeal approach without an enterprise wide coordinated strategy. We also need more clarity on definitions, so everyone knows what to protect and how. As we continue to work with DOD, Congress and other stakeholders to address this threat I hope that we can continue to progress towards a more unified approach across the Department while also providing DOD contractors the opportunity to provide inputs on proposed approaches and facilitate the most effective, efficient allocation of resources to accomplish the common goal of greater cybersecurity.

Again, thank you for the opportunity to meet today and discuss these issues of vital importance to our nation's warfighters and industry. I look forward to your questions.

###