STATEMENT BY

MR. JESSE SALAZAR
DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR INDUSTRIAL POLICY

BEFORE THE SENATE ARMED SERVICES COMMITTEE
SUBCOMMITTEE ON CYBERSECURITY

ON

DEFENSE INDUSTRIAL BASE CYBERSECURITY

MAY 18, 2021

EMBARGOED UNTIL RELEASED BY THE SENATE ARMED SERVICES COMMITTEE

Chairman Manchin, Ranking Member Rounds, and distinguished Members of the Cybersecurity Subcommittee, thank you for the opportunity to testify on the importance of mitigating cybersecurity risk within America's defense industrial base (DIB). I am pleased to be here with Rear Admiral Bill Chase, Deputy Principal Cyber Advisor to the Secretary of Defense. I assumed the position of Deputy Assistant Secretary of Defense for Industrial Policy three months ago with an aim to build a healthier and more resilient industrial base that deters conflict, protects our national security, and enables global economic leadership.

The U.S. defense industrial base remains the envy of the world because of its sophistication, diversity, and capacity to innovate for the needs of the warfighter. Every day, people across this country are working to ensure that our armed forces have every advantage they need.

In my role, I work with colleagues across the Department to ensure that we are meeting our responsibility to protect American industrial capabilities and the companies and people that make them possible. Increasingly sophisticated, well-resourced, and pervasive cyber-attacks, including state-sponsored espionage, are threatening the United States and the rules-based order on which the global economy relies. That's why DIB cybersecurity remains a top priority. I consider this Committee to be a critical partner in these efforts.

Current threat landscape

Recent examples of malicious cyber activity have shown that our adversaries are evolving their exploitation of cyberspace to steal sensitive, albeit unclassified, information from the government and the industries who make our work possible. Fallout continues from Russia's Solarwinds cyber espionage campaign that breached 16,800 users through exploitation of what was observed to be a routine software update. Advanced persistent threat groups have recently attacked U.S. defense targets through security flaws in VPN devices and email exchange servers.

Highly capable and motivated adversaries are maneuvering to infiltrate where they can, especially where they see weak links in the supply chain. Protecting the complex network of interconnected firms that comprise the defense industrial base has never been more challenging. The average American aerospace company today has about 200 tier 1 suppliers. The second and

third tiers of the supply chain may be comprised of more than 12,000 companies, offering numerous pathways for adversaries to access sensitive private and public sector information. Nearly all firms in the third and fourth tiers of the supply chain, or 74% of the defense industrial base, are small businesses according to the Department's contracting data.

Having worked in the private sector, I can attest that these small businesses work hard to stay profitable. Few, if any, have a full-time IT or cybersecurity professional on staff. Predatory cyber actors are more likely to target these smaller firms to gain access – a task which they find more difficult with larger contractors. Moreover, we are in the dawn of the Fourth Industrial Revolution, so entry points into the defense industrial base are multiplying as firms invest in more digital capabilities, from cloud-based data management platforms to IoT-enabled factories to remote-work technology. The same pace of technological advancement and digital connectivity that contributes to America's global military edge is also challenging us in cyberspace.

A 2020 CSIS-McAfee report estimated that global losses from cybercrime now total over $1 trillion annually. Nearly 80% of senior IT and security leaders believe their organizations lack sufficient protection against cyberattacks, despite increased IT security investments made in 2020. In fact, the number of breaches in 2020 set a record, hitting a level greater than the previous 15 years combined. On average, data breaches cost companies nearly $4 million in 2020, and resulted in increased downtime, reduced efficiency, and long-term reputational damage.

To frustrate, disrupt, and defeat adversaries' efforts to infiltrate our cyberspace, the Department must ensure that the DIB continues to build cyber resilience. Our challenge is to determine how to prioritize limited resources to manage cyber risk across the entire attack surface -- from the Department and the primes to the subcontractors delivering major weapons systems and small businesses that manufacture components. To protect the whole supply chain, the DoD must promote a culture of cyber-resilience by including requirements for appropriate and effective cybersecurity measures in our contracts and ensuring that these contractual requirements are being met. Because of the national security interests at stake, we will continue seeking

assurances that firms are meeting these requirements and safeguarding the controlled unclassified and classified national security information entrusted to them. A combination of education, information-sharing, and cybersecurity tools and services at a reasonable cost can help us achieve these aims, especially for small- and medium-sized businesses.

Cybersecurity Maturity Model Certification Program

As Rear Admiral Chase outlines in his testimony, the Department has numerous programs and thousands of personnel working to improve the cybersecurity posture of the DIB. I have recently assumed oversight of one key component of this expansive effort: the Cybersecurity Maturity Model Certification program (CMMC). CMMC operationalizes the Department's commitment to incorporate cybersecurity into the defense acquisition system, with a focus on protecting controlled unclassified information, particularly the controlled technical information, which makes our warfighting advantages possible. As this sub-committee has underscored through its leadership and legislation, security is foundational to acquisition and should not be traded along with cost, schedule, and performance.

In connection with the CMMC program, the Department has put in motion a substantial effort to update acquisitions processes and practices to manage information and associated cybersecurity requirements at all levels in the supply chain, from the prime contractors down to the smallest firms delivering component parts. Developed in coordination with DoD stakeholders, University Affiliated Research Centers (UARCs), Federally Funded Research and Development Centers (FFRDC), and industry, the CMMC framework has three broad objectives that are critically important to the protection of sensitive information:

1. **To incorporate a unified set of cybersecurity requirements into acquisition processes and contracting language.** Recognizing that cybersecurity should not be "one-size-fits-all," the program includes several levels of cyber requirements, that allow flexibility to apply requirements appropriate to the defined sensitivity level of information at issue.
2. **To provide the Department assurance, via external assessment, that all contractors and subcontractors participating in a given award meet mandatory cybersecurity requirements.** The certification framework also facilitates the Department's ability to

hold prime contractors accountable for ensuring that their suppliers are, in fact, implementing appropriate cybersecurity requirements.

3. **To develop supporting resources, information, and training to help contractors improve cyber readiness and comply with the Department's requirements.**

The CMMC program represents a major leap forward in the Department's approach to cybersecurity, and it has already led to DIB companies taking action to improve their cybersecurity posture.

In contrast to self-attestation, CMMC enables increased visibility into whether cybersecurity requirements are being met and passed on to subcontractors, requires discipline and awareness around the type of information that is flowed down through the supply chain, and provides the Department with a mechanism to ensure that contractual cybersecurity requirements are fulfilled.

As the Department's most ambitious cybersecurity program for the DIB to date, CMMC also raises additional policy and implementation considerations. I am grateful to the organizations and individuals that submitted more than 850 comments in response to the DFARS interim rule establishing CMMC. In addition, my office has hosted more than a thousand conversations with members of Congress and Congressional staff, DIB companies and industry associations, and international allies and partners to understand further the challenges and outstanding questions the Department must address in navigating a path forward on DIB cybersecurity. In March, Deputy Secretary Hicks directed an internal programmatic assessment of CMMC which engaged cybersecurity and acquisitions stakeholders from across the Department to complement the feedback we have received from external stakeholders. Our completed 'pathfinders' and upcoming pilot development phase will further help us understand the best ways to achieve our goals through program implementation.

The Department is currently working with internal stakeholders on adjudicating these inputs.

Our outreach and analysis on the best pathways to implement the policy objectives of CMMC are ongoing, and we will continue to engage with Congress, industry, international partners, and other stakeholders as we chart the way forward. I, along with senior colleagues in the Department, are particularly focused on the following policy considerations:

1. *Managing costs of cybersecurity for small businesses*

About three-quarters of the DIB is comprised of small businesses that produce many innovative capabilities and emerging technologies. This segment is already under immense pressure – according to federal procurement data, the number of small businesses in the DIB has shrunk by more than 40% over the last decade against the prevailing forces of consolidation and concentration among defense contractors. Small businesses have told us loud and clear that they face additional resiliency issues in the face of COVID-19. According to a Defense One survey, one in seven believe they will never return to pre-pandemic levels of business performance. The Department's approach to cybersecurity must balance the need for accountability with a recognition of the challenges facing small businesses.

2. Clarifying cybersecurity regulatory, policy and, contracting requirements

As part of the CMMC certification process, the Department needs to de-conflict and streamline multiple cybersecurity requirements to prevent duplicative assessments. This includes providing clear guidance on the alignment of the NIST SP 800-171 DoD Assessment Methodology and CMMC, as they pertain to safeguarding controlled unclassified information (CUI), as well as the requirements and assessment approach for contractors that use cloud service provider offerings. Moreover, the Department is committed to working with our allies and international partners to better understand how the CMMC framework compares with other nations' cybersecurity requirements and better align these requirements to help protect the Department's mission critical supply chain.

3. Reinforcing trust and confidence in the maturing assessment ecosystem

CMMC's implementation process, which requires companies to obtain a cybersecurity certification once every three years, is an important, first-of-its-kind effort to validate that the DIB is meeting the requisite security requirements. The Department must ensure that we can operationalize our requirements by confirming there are sufficient numbers of assessors to deliver independent, rigorous, and timely assessments to support our acquisition requirements. Further, the DoD must ensure there are clearly defined roles and responsibilities, standards of conduct, and audit mechanisms governing relationships with private sector entities within the external assessment system.

Broader efforts to protect the cybersecurity of the defense industrial base

In addition to CMMC, which is primarily focused on holding companies accountable for the implementation of rigorous cybersecurity programs, the Department is pursuing a number of complementary initiatives that enable and support companies in meeting our requirements. To help address some of the challenges I laid out above regarding cost and implementation, and particularly to support small businesses to shore up their cyber defenses, my office is exploring, in partnership with Rear Admiral Chase, how we can expand and increase DIB firms' access to:

- Education and training programs such as Project Spectrum. Supported by the Industrial Policy office, this program offers cybersecurity online courses, training videos, risk assessments, and other resources to help small companies improve cyber readiness and comply with DoD requirements.
- Cyber threat information sharing programs such as the Defense Industrial Base Cybersecurity (DIB CS) program, which crowdsources information about cyber incidents from individual DIB companies and provides centralized threat analysis back to the DIB in order to reduce collective risk.
- Cybersecurity-as-a-service programs, such as "Protective DNS", as described in detail by Deputy PCA Chase, and the Cyber Resilience Analysis program (CRA). CRA is managed by the Department of Defense Cyber Crime Center (DC3) and conducts facilitated assessments of DIB firms to assist in reviewing and assessing cyber threats when requested.

Ultimately, the Department's goal is to ensure that all members of the defense industrial base, from the largest prime to the smallest business, embed cybersecurity into core operational and business practices and build a culture of cybersecurity and cyber resilience to keep pace with the rapidly evolving threat.

Path forward

I, along with other senior leaders in the Department, are devoted to further strengthening and operationalizing this program.

Over coming weeks and months, we will incorporate the inputs we have received with an eye toward continually increasing DIB cybersecurity, minimizing barriers for small businesses, maintaining public trust, and operationalizing this vital effort. Our adjudication of these inputs will be guided by two central principles.

First, we will continue to emphasize requirements to protect controlled unclassified information that is shared with and developed by the DIB. The Department should be resolute in its commitment to safeguarding warfighters and the systems they need to win.

Second, we will seek ways to implement these requirements without creating unnecessary barriers to entry or costs that discourage the most innovative companies from joining the DIB. By working with industry, Congress, international partners, and other key stakeholders inside and outside the Department, we will continue to strengthen this program with an aim to frustrate, disrupt, and defeat our adversaries' efforts in cyberspace.

Cyberspace has never been more important, nor more contested, than it is today. Together, we face an enormous challenge in securing the DIB in the cyber domain. Still, the United States of America does not get dissuaded by the prevalence of the challenges we face; we always rise to meet any and all threats to the nation.

Thank you for providing me an opportunity to testify before you today. I look forward to your questions.