**STATEMENT BY**

**REAR ADMIRAL WILLIAM CHASE**
**DEPUTY PRINCIPAL CYBER ADVISOR TO THE SECRETARY OF DEFENSE**
**DIRECTOR OF THE PROTECTING CRITICAL TECHNOLOGY TASK FORCE**

**BEFORE THE SENATE ARMED SERVICES COMMITTEE**
**SUBCOMMITTEE ON CYBERSECURITY**

**ON**

# DEFENSE INDUSTRIAL BASE CYBERSECURITY

**May 18, 2021**

Chairman Manchin, Ranking Member Rounds, thank you for your invitation to appear again before this subcommittee. The last time I was in the Senate, I provided testimony on the Department's zero trust cybersecurity initiative. Today, I am here as the Deputy Principal Cyber Advisor to the Secretary of Defense, representing my civilian senior, the Principal Cyber Advisor, who is responsible for driving implementation of the DoD Cyber Strategy, oversight of U.S. Cyber Command, and, pursuant to section 1724 of the National Defense Authorization Act for Fiscal Year 2021, serving as the coordinating authority for Defense Industrial Base, or DIB, cybersecurity.

My remarks today reflect two complementary imperatives: the need to improve DIB cybersecurity across the board and at scale and the need to focus protection resources on programs of particular importance. The Department has many programs and thousands of personnel working on DIB cybersecurity in some form or fashion. Today, I will cover a slice of the policies, plans, and activities that are making an impact and the actions that we are taking both to raise the costs of committing cyber espionage and actively defend the Department's most critical programs and technologies. Neither the Department nor the DIB will ever be able to secure industry's networks and controlled unclassified information completely, but our goal over the short, medium, and long terms is to complicate and frustrate adversary planning and operations so that our adversaries cannot act with impunity or at scale.

Since at least 2006, the Department has recognized and taken action to diminish the threat of adversary cyber espionage of the Defense Industrial Base. Still, that threat continued to grow, and, in 2018, the Department of Defense faced a threat to its military advantage by determined adversaries and their intent to steal plans, documentation, designs, and intellectual property for key weapon systems. Our adversaries had limited access to key networks on the

well-defended Department of Defense Information Network (DODIN) but were considerably more successful in compromising the unclassified networks of the DIB, particularly those of small- and medium-sized subcontractors, where much of the same valuable data resides. Cyber espionage is, in many cases, the preferred espionage vector for our adversaries, allowing for persistent access to the Department's data at low-cost and permitting remote operations at scale. Adversaries are, however, also employing foreign intelligence officers and non-traditional collectors—using academic researchers to gain technical insight, for example—importing dual-use technologies, and using foreign direct investment to acquire defense companies, promising startups, and companies adjacent to military bases and ranges.

In response to this threat, the Department established the Protecting Critical Technology Task Force (PCTTF) in 2018, which, across four lines of effort, aimed to improve the cybersecurity of the Defense Industrial Base, secure the Department of Defense research and development enterprise, stop technology leakage through export and foreign ownership, and impose costs on adversary intelligence campaigns. The PCTTF, the Under Secretary of Defense for Acquisition and Sustainment, the Under Secretary of Defense for Research and Engineering, the Under Secretary of Defense for Intelligence and Security, the Department of Defense Chief Information Officer, and the Military Services all realized that the status quo means of ensuring DIB cybersecurity and the protection of sensitive controlled information on DIB systems were fundamentally inadequate. The Defense Federal Acquisition Regulation Supplement was amended in 2013 to require contractors—and subcontractors, to whom these requirements were to be passed down—to safeguard covered defense information residing on or transiting through a contractor's internal information system or network and to provide adequate security for such systems, including implementing the controls established in NIST Special Publication 800-171.

The contract clause also established reporting requirements for cyber incidents affecting such systems or the covered defense information therein.

These contractual requirements often appeared to be addressed in a perfunctory manner, and the Department identified the need to enhance DoD's ability to ensure that such cybersecurity requirements were, in fact, being implemented. A Chief Information Security Officer position was created within the Office of the Under Secretary of Defense for Acquisition and Sustainment to help drive change in the way cybersecurity risk is addressed in connection with the Department's acquisition efforts. In conjunction with the Carnegie Mellon Software Engineering Institute and Johns Hopkins University Applied Physics Laboratory, the Under Secretary of Defense for Acquisition and Sustainment created the Cybersecurity Maturity Model Certification model, and later established the CMMC program, which involves use of accredited and trained third-party assessors to assess contractors' and subcontractors' cybersecurity prior to contract award. This program addresses two critical issues: first, by only awarding contracts to contractors with a valid CMMC certification, awarded in the last three years, the program incents contractors to, in fact, implement needed cybersecurity measures; and second, the program flows down the requirements to ensure subcontractors are similarly certified.

The Chief Information Security Officer for Acquisition and Sustainment, who is responsible for the CMMC program, reports to Mr. Salazar as Deputy Assistant Secretary of Defense for Industrial Policy, so I will defer to his expertise for further discussion of the CMMC. From a cybersecurity perspective, we recognize the gap the CMMC is intended to address and also the concerns that industry, particularly small businesses, has raised regarding: the investments required to achieve CMMC compliance prior to contract award; the need to deconflict and streamline multiple cybersecurity standards and assessments; and the uncertainty

surrounding the CMMC ecosystem. Although we should not apologize for imposing cybersecurity requirements to protect key information regarding our warfighting systems, we must also be pragmatic and avoid imposing unnecessary compliance costs on industry and sacrificing innovation as a result. We must focus our attention and resources on the supply chains of the Department's most critical programs and program elements, systematically segmenting risk and then limiting these programs' exposure to cyberattacks. For the DIB as a whole, we must consider provisioning cybersecurity capabilities in partnership with key cybersecurity, information technology, and Internet-related players in industry.

Pursuant to these imperatives, the Department is taking a multi-faceted approach towards ensuring the cybersecurity of the Defense Industrial Base. DoD CIO is in the process of expanding its DIB Cyber Security information-sharing program through the Defense Cyber Crime Center (DC3) under the U.S. Air Force. Although this program was designed to share indicators of compromise and malware analysis services with cleared defense contractors—those members of the industrial base that have security clearances and access to classified information—the DoD CIO is working to amend relevant regulations to expand the program to include non-cleared defense contractors, thus enabling small- and medium-sized contractors to receive important information, including the same signatures, malign IP addresses, and threat advisories that the larger cleared primes receive as part of the program. DC3 is also expanding the services available to the DIB, piloting efforts such as penetration testing to address contractors' external-facing vulnerabilities and an adversary emulation program.

The National Security Agency (NSA) is also conducting a number of pilots, leveraging authorities to share unique, actionable threat information and cybersecurity guidance with members of the DIB and their service providers and to provide unique cybersecurity capabilities

to the DIB, among the most promising of which is the provision of free and secure Domain Name System (DNS) lookup services to the DIB. The DNS is colloquially referred to as the phonebook of the Internet, translating readily remembered website names (e.g., defense.gov) to IP addresses appropriate for internet routing. The NSA is offering this cybersecurity service—called Protective DNS, or pDNS—in partnership with an advanced commercial DNS provider and is currently enrolling members of its industrial base. This capability combines a commercial DNS sensor architecture with real-time analytics to quickly understand malicious activity targeting the DIB and to deploy immediate countermeasures. The efficacy of this service has been widely demonstrated—it does not require access to internal contractor networks and has the potential to prevent or disrupt adversary cyber exploitation activities.

I am especially excited about a number of these pilots in which cybersecurity capability is directly offered to contractors and subcontractors, because they offer the promise of cost-efficient, scalable solutions that can be provided to contractors of any size or profitability. Unlike approaches that depend on the DIB's sensoring, instrumentation, configuration, and operation of cybersecurity tools on their own networks, a number of the initiatives being piloted by the NSA and DC3 include direct cybersecurity services provisioned and managed by cybersecurity and IT service providers. This approach institutionally buys down cybersecurity risk across entire industry segments rather than relying on individual small- and medium-sized businesses to defend their networks as if they were large prime contractors.

Not all of these technical concepts require the government to provide such services—industry stakeholders, through the DIB Sector Coordinating Council, are also piloting a number of concepts that could be applied across their supply chains, including the provision of secure e-mail, secure cloud environments, and sensors for subcontractor networks. We must continue to

pilot these concepts of operation and capabilities and then scale the successful ones. The direct provisioning of cybersecurity capabilities to contractors, including the provisioning of secure environments for development and storage of controlled unclassified information, is incredibly promising.

The Department of Defense counterintelligence community—the Defense Counterintelligence and Security Agency and Military Department Counterintelligence Organizations—is also making significant progress in reducing cyber threats to the DIB. Each entity is growing and improving its programs and posture to counter the cyber threat, proactively detecting adversary cyber activity, working with partners in the Intelligence Community to address intelligence gaps, and integrating law enforcement, counterintelligence, and intelligence situational awareness and operations. Their technical modernization programs are improving interoperability and collaboration across the community through the Collect, Analyze, Disseminate, and Operationalize initiative. This is an important and underemphasized component of the Department's DIB cybersecurity plans, policy, and programs. Counterintelligence has a mutually beneficial relationship with security, and the community is investing increasingly in programs and partnerships that allow for improved visibility of adversary activity at scale. This progress is matched by activities across the U.S. Government, including the NSA, the Federal Bureau of Investigation, other elements of the Intelligence Community, U.S. Cyber Command, and the Cybersecurity and Infrastructure Security Agency, to detect cyber targeting and defend the DIB.

Most of the Department's programs and policies to protect the DIB are ultimately implemented through program managers in the DoD Components, particularly within the Military Departments and Services. Each of the Military Services has developed programs,

policies, and guidance and apportioned resources for program managers to be able to evaluate and address the cyber risk posed to their supply chains more effectively. Although this progress is often invisible at the Office of the Secretary of Defense level, it is absolutely crucial. The Military Services—and DoD Components with acquisition authorities like the Missile Defense Agency and U.S. Special Operations Command—ultimately issue contracts, manage programs, and implement policy. We must ensure that they have a clear grasp of the persistently evolving nature of the cyber operating environment, an understanding of the types of risks their programs and systems are subject to, and the steps they must take to drive DIB cybersecurity.

The Under Secretary of Defense for Research and Engineering, the Under Secretary of Defense for Acquisition and Sustainment, the Under Secretary of Defense for Intelligence and Security, and the Protecting Critical Technology Task Force have each played a significant role in shifting the Department's culture and have taken a number of steps to ensure that program managers are required and able to address cybersecurity risks. The Under Secretary of Defense for Research and Engineering has reinforced responsibilities and procedures for science and technology managers and the engineering workforce. These procedures enable and protect technology innovation in our warfighting capabilities through superior program protection practices and secure, cyber-resilient engineering design. The Under Secretary of Defense for Acquisition and Sustainment has developed acquisition policy to establish a number of program manager-specific requirements for cybersecurity, program protection, and supply chain risk management. The Under Secretary of Defense for Acquisition and Sustainment is also modernizing program manager training, education, and guidebooks to ensure that program managers account for cybersecurity in all phases of the acquisition lifecycle. The Under Secretary of Defense for Intelligence and Security has implemented the controlled unclassified

information program and continues to carry out assessments of cleared defense contractors via the National Industrial Security Program. The Protecting Critical Technology Task Force has established and coordinated a Critical Programs and Technology list to identify clearly and drive components to protect the Department's most important science, technology, and acquisition programs.

Progress in DIB cybersecurity is also being driven from industry. Industry stakeholders, including large defense prime contractors, in addition to conducting the pilots mentioned earlier, have been key partners in reinforcing their own supply chain security programs, making resources available to their subcontractors, and working with Department of Defense program managers to ensure the security of their supply chains. The Department relies on its prime contractors to ensure the sanctity and operational security of critical information integrated in its programs—close coordination, cyber-conscious program management, and the establishment of appropriate incentives are critical.

Last year's National Defense Authorization Act requires that the Principal Cyber Advisor serve as the coordinating authority for DIB cybersecurity issues in the Department of Defense. This is a familiar role for the Office of the Principal Cyber Advisor (OPCA) as the coordinator and facilitator of numerous initiatives germane to cyberspace, and we are excited to take it on. The OPCA will leverage existing governance fora and coordination mechanisms to identify gaps and redundancies across the Department's DIB cybersecurity programs and raise barriers and critical issues to the attention of the Deputy Secretary of Defense, the Under Secretaries of Defense, the Joint Staff, and the Military Departments and Services so that they may address them.

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