STATEMENT OF

MS. LAURIE BUCKHOUT

PERFORMING THE DUTIES OF ASSISTANT SECRETARY OF DEFENSE FOR CYBER POLICY

TESTIMONY BEFORE THE

HOUSE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON CYBERSECURITY, INNOVATIVE TECHNOLOGIES, AND INFORMATION SYSTEMS

MAY 16, 2025

Introduction

Chairman Bacon, Ranking Member Khanna, and members of the Committee, thank you for the invitation to be here today and discuss the Department of Defense (DoD)'s cyber posture. It is an honor to share the stage with representatives from U.S. Cyber Command. Their leadership is crucial as we navigate the complexities of the evolving cyber domain and I value the ongoing partnership between our organizations – it is a relationship built on mutual respect and a shared commitment to national security, guided by the vision of peace through strength that President Trump has articulated.

I am deeply grateful by the opportunity to serve as the Deputy Assistant Secretary of Defense (DASD) for Cyber Policy and perform the duties of Assistant Secretary of Defense (ASD) for Cyber Policy. I come to this role after more than 25 years in military service, including a 2003 task force assignment in Iraq, and I could not be prouder to once again be serving my country under our 29th Secretary of Defense, Pete Hegseth.

In my role Performing the Duties of ASD for Cyber Policy, I provide comprehensive oversight of DoD's cyber policies, advancing our strategic approach to cyberspace and ensuring our readiness to confront emerging cyber threats. Mr. Chairman, I look forward to working with you and this Subcommittee to achieve these goals.

The President has nominated Ms. Katherine Sutton to serve as the ASD for Cyber Policy. I look forward to supporting her as the DASD for Cyber Policy, should she be confirmed. I also want to acknowledge the hard work and dedication of the professionals in the Office of the ASD for Cyber Policy. They are the backbone of our efforts.

Security Environment

The United States faces a strategic environment of heightened complexity and risk. This environment is defined by the vulnerability of our Homeland to the evolving capabilities of near-peer competitors and other adversaries, who pose new and alarming threats across both kinetic and non-kinetic spheres. Cyberspace, a domain essential for global connectivity, communication, and innovation, has also become a contested battlespace. Malicious actors, including nation-states and criminal organizations, are blurring the lines between traditional

adversaries, and creating novel challenges that demand a comprehensive and coordinated response, both domestically and internationally.

Of particular concern is the increasing willingness of adversaries to use cyber capabilities not only for espionage but also to gain access and preposition for disruptive actions. The interconnectedness of our digital infrastructure means that vulnerabilities in one area can have cascading effects across multiple sectors. This digital infrastructure also underpins other essential functions of our Nation, from how Americans communicate with loved ones, to how we navigate, to how our economy functions at its core, underscoring the need for enhanced cybersecurity and proactive risk mitigation.

China: The People's Republic of China (PRC) remains DoD's foremost challenge in cyberspace. China possesses an extensive cyber workforce and supporting ecosystem that contribute to the Chinese Communist Party's (CCP) malicious cyber activities. China's ongoing cyber espionage actions target U.S. networks to pilfer intellectual property, acquire research data, and generate sensitive insights into U.S. Government and corporate activities. This sustained pursuit of technological and economic advantage poses a long-term threat to our national competitiveness and military dominance. The Secretary of Defense has directed DoD to prioritize resources towards the most lethal and effective capabilities required for the Joint Force to defend the Homeland and deter China, a strategic imperative in which cyberspace plays a foundational role.

The activities of China's "Volt Typhoon" cyber actor group remain a primary DoD concern and focus area for protecting the digital infrastructure supporting Joint Force operations. Public disclosure of Volt Typhoon activities in mid-2023 highlighted China's persistent efforts to gain and maintain access within multiple U.S. critical infrastructure sectors. Volt Typhoon actors employ stealthy techniques, including extensive network reconnaissance and obfuscation within normal network activity, enabling them to remain undetected for extended periods. Further, the discovery late last year of the Chinese intrusion set known as "Salt Typhoon" on multiple U.S. and global telecommunications providers underscores the pervasiveness of China cyber activity within critical infrastructure. The U.S. Government, in collaboration with allies and partners, is actively addressing these threats.

The CCP continues to invest in its cyber workforce and capabilities, including recruitment, training, and research into emerging technologies such as artificial intelligence and quantum computing. DoD must counter these advancements through investments in our own advanced technologies, offensive and incident response capabilities, enhanced cybersecurity and resilience, and strengthened collaboration between DoD and civilian agencies. These actions are crucial to preserving essential warfighting functions and developing offensive cyber capabilities to deter China, our most consequential opponent in strategic competition.

Russia: The Russian Federation continues to pose a significant cyber threat to the United States and our allies and partners, employing cyber capabilities to conduct espionage, influence the information environment, and execute cyber attacks. Russia's cyber operations are often integrated with its broader geopolitical objectives, aiming to sow discord and project power on the global stage. The Kremlin views cyberspace as an essential tool for advancing its strategic aims and challenging United States national interests.

While Russia's cyber operations continue to support military operations in Ukraine, it maintains campaigns against the United States and North Atlantic Treaty Organization (NATO) allies. Russia leverages these activities to refine its cyber tradecraft and integrate cyber operations with traditional military operations. The United States must be prepared to counter Russian activities affecting United States vital national interests across all domains, while increasing burden-sharing with allies and partners to address these shared threats globally.

Other Threat Actors: The Islamic Republic of Iran leverages cyber capabilities to conduct operations against regional adversaries and amplify anti-Western sentiment globally. Iran is adept at casting a wide net with its cyber operations, leveraging its capabilities to sow discord and managing the information space to its advantage. While regionally focused, Iran maintains capabilities to conduct espionage and cyberattacks against the United States and our partners to achieve political and military objectives. For example, last year, Iran sought to compromise multiple U.S. and partner critical infrastructure sector networks and deepened its partnerships with countries like Russia to enhance their technical prowess.

The Democratic People's Republic of Korea (DPRK) increasingly utilizes cybercrime, particularly cryptocurrency theft, to finance its weapons programs and is becoming more effective at hiding those funds through digital money laundering activities. The DPRK also

conducts espionage activities against defense, aerospace, and nuclear-related entities to acquire sensitive information and intellectual property.

For-profit cybercriminals, some operating as proxies or agents of nation-state adversaries, continue to target U.S. critical infrastructure, particularly networks with limited cyber defenses. The rise of Ransomware-as-a-Service (RaaS) platforms has lowered the barrier to entry for cybercriminals and increased the threat posed by these actors.

Finally, the pervasive threat of transnational criminal organizations (TCOs) adds another layer of complexity to this security environment. These TCOs and foreign terrorist organizations (FTOs), including Mexican drug cartels, exploit the anonymity and speed of cryptocurrencies to launder illicit profits and evade detection. They exploit vulnerabilities along America's borders to import fentanyl and their suppliers in China engage in elaborate schemes involving all shipping modalities, and coded communication on dark web marketplaces to supply FTOs in Mexico with precursor chemicals. DoD's founding mission is homeland defense; we will continue to commit fully to our role protecting the territorial integrity of the United States by countering the dangerous intersection of cyber capabilities and TCO operations.

Role of the ASD for Cyber Policy

Within this complex and varied threat environment, the Office of the ASD for Cyber Policy plays a central role in integrating national cyber policy with DoD policies. This office provides guidance and oversight for DoD cyberspace activities related to foreign cyberspace threats, including international cooperation and engagement with foreign partners and international organizations, as well as the implementation of DoD cyberspace plans related to cyberspace forces, capabilities, and their employment.

Designated by statute as the Principal Cyber Advisor (PCA) to the Secretary of Defense, the ASD for Cyber Policy is vested with oversight responsibilities for U.S. Cyber Command's authorities granted under Title 10, Section 167(b) of the U.S. Code. A primary responsibility under these PCA authorities is the oversight and support of the organization and readiness of cyber operations forces assigned to U.S. Cyber Command. Leveraging statutory requirements within the Fiscal Year 2023 National Defense Authorization Act (NDAA), this office collaborated with U.S. Cyber Command and DoD stakeholders to assess and refine the

generation of DoD cyber forces. Together, we are working to ensure that DoD's cyber activities are aligned with national security objectives, that we are effectively deterring and responding to cyber threats, and that we are building strong relationships with our allies and partners.

Strategic Lines of Effort in Cyber

Our strategic lines of effort are oriented around Secretary Hegseth's three priorities: homeland defense, lethality, and warfighting. We will work to increase the number of highly skilled professionals dedicated to securing cyberspace and reinforce the capacity to deter and respond swiftly and decisively to cyberattacks. This necessitates a shift from a reactive posture to a more proactive and assertive approach. To that end, we are concentrating our efforts in three key areas:

Reestablishing Deterrence & Securing the Homeland: Our foremost priority is to protect and defend the American homeland against aggression in cyberspace. We ensure our cyberspace operations forces have the resources, authorities, and strategic direction they need to contribute to deterrence; and, if necessary, defend against and defeat cyber threats from abroad. Every day, these forces defend against our adversaries in cyberspace, disrupting malicious cyber threats before they reach our domestic networks and demonstrating our strength to our adversaries. We zealously defend against cyber threats to our Homeland and reserve the right to respond in the time, place, and domain of our choosing.

The American homeland is further strengthened against cyber threats by actions we take to make our systems and networks more resilient and easier and cheaper to defend. Consistent investments in technology modernization and cybersecurity best practices will reduce our vulnerability to adversary attacks and free up our defenders to identify and defeat the most sophisticated cyber threats.

Enhancing our national cyber resilience requires collaboration and partnership with stakeholders across the cyber ecosystem. Working with other Federal partners, we use our unique authorities and capabilities to identify and mitigate vulnerabilities, share threat intelligence, and develop effective incident response plans. DoD serves as the Sector Risk Management Agency for the defense industrial base (DIB), and we prioritize activities to help DIB organizations enhance their cybersecurity posture and defend themselves against dynamic

cyber threats. We also support whole-of-government initiatives to strengthen the resilience of critical infrastructure across the nation. This is particularly important for defense critical infrastructure in sectors such as communications, energy, and water and wastewater, which directly enable our warfighting capabilities.

We also seek to use cyberspace operations to enable compounding kinetic and non-kinetic effects to deter and defeat our adversaries in wartime. Executing cyber options in a time of conflict requires actions today to gather intelligence, generate capabilities, and enhance our plans. We support campaign and contingency planning to enable joint plans and operations that maximize the impact of our unique capabilities in cyberspace. By developing a range of cyber options, we can deter our adversaries from aggression in cyberspace today and ensure we have the ability to respond effectively in times of conflict.

Restoring the Warrior Ethos: DoD's mission is to win the Nation's wars. To do this, we must have a lethal fighting force that rewards excellence and readiness. Our cyber workforce is our most valuable resource in the digital battlespace. To maintain our advantage in the face of evolving cyber threats, we must prioritize recruiting, training, and retaining the most talented individuals. An optimized force generation model is key to how we develop and sustain a world-class cyber force. We are not simply expanding the ranks; we are building a highly specialized cadre of cyber professionals that possess mastery in the cyber domain. This requires several enabling factors.

First, recognizing the critical need to attract and retain top-tier talent, we are actively exploring competitive compensation packages and career advancement opportunities to ensure our cyber workforce remains highly motivated and engaged. To further bolster our capabilities, we are refining unit readiness cycles to guarantee our forces are adequately trained, equipped, and prepared for rapid deployment.

Finally, to expedite the development and implementation of cutting-edge cyber capabilities, we are cultivating a culture of innovation, connecting our cyber operators with leading researchers, technologists, and industry partners. We will ensure our forces have access to the most advanced tools and technologies, allowing them to stay ahead of our adversaries.

Rebuilding our Military: The Department is strengthening the military by cutting excess and refocusing the DoD budget to put us on a ready footing to deter our enemies and fight for peace. Given the increasingly dangerous strategic environment we face and the resource constraints we can no longer ignore, DoD is prioritizing cyberspace capabilities that directly enable warfighter lethality and decision advantage.

Operations in cyberspace are critical to the Joint Force's ability to fight and prevail in conflict, particularly against technologically sophisticated threats. This starts with ensuring that our adversaries cannot use cyberspace operations to degrade our conventional capabilities. We continuously assess the capabilities and intentions of our adversaries in cyberspace, and we use these insights to improve the cybersecurity and resilience of DoD's own networks and systems and increase our lethality. U.S. Cyber Command plays a critical role in enabling our advantage in cyberspace and ensuring other combatant commands can execute their plans and operations with confidence.

In many cases, we can generate highly effective capabilities that incorporate low-cost solutions from the private sector. DoD is enhancing its acquisition pathways to improve the ways we buy software and modernize our information technology, including through new partnerships with non-traditional suppliers. Our private sector partners have unique visibility into adversary threat activity that, when shared with the U.S. Government, can enable us to use our authorities and capabilities to make the entire community safer. We further recognize that information sharing must go both ways, and we continuously look for opportunities to get timely, actionable information about cyber threats and vulnerabilities into the hands of organizations facing these threats every day. U.S. Cyber Command's UNDER ADVISEMENT program is one such tool for increasing threat information sharing, allowing system owners and operators to close vulnerabilities before they can be exploited by cyber threat actors.

Lastly**,** we benefit from working closely with allies and partners around the world, particularly those with advanced cyber capabilities. These advanced partners have an important role to play in defending their own networks against adversary cyberattacks, both to prevent attacks on their own citizens and to prevent their infrastructure from being used to launch intrusions of U.S. systems. The strength of DoD is our unity and shared purpose. We will continue to engage with our Allies and partners in a manner that prioritizes American national

security and reduces cyber threats worldwide to advance the President's priority to end wars responsibly and reorient to key threats.

Looking Forward in 2026

I am grateful for continued Congressional support for legislation enabling an update to our force generation model and the Cyber Excepted Service, as well as key provisions in prior NDAAs that have enhanced our operational effectiveness, such as the clarification of the Traditional Military Activities exemption under Title 50 of the U.S. Code, and streamlined capabilities development, such as U.S. Cyber Command's Enhanced Budget Control. This support is essential to mission success, and we look forward to demonstrating the tangible outcomes of this support in the 2026 Cyber Posture Review.

Success in this challenging environment necessitates a Joint Force that is ready, capable, and resourced to operate effectively in cyberspace. The scale and urgency of cyber threats demand clear prioritization and sound strategic choices. DoD must rebuild the military and revitalize America's defense industry rapidly but at a reasonable cost, consistent with principles of fiscal responsibility. Achieving this objective requires sustained investment in our personnel and our capabilities.

Our people remain our most important asset in cyberspace. Recruiting, retaining, developing, and rewarding the highly skilled individuals on the front lines of cyber defense is paramount. The principal objective of the cyber force redesign planning effort is to enable cyber warfighters to achieve mastery in the cyber domain, and they remain the highest priority.

I acknowledge and appreciate the recent allocation of additional budgetary authority to U.S. Cyber Command and the PCA, and I am committed to implementing these authorities in close partnership with U.S. Cyber Command. The issuance of the inaugural Cyber Operations Programming Guidance (COPG) provides a framework for DoD to prioritize program investments in cyber capabilities, enhancing oversight of U.S. Cyber Command's budget and enabling more comprehensive certification of Service and Command budget requests.

Development of this year's COPG will emphasize investments aligned with DoD initiatives to integrate artificial intelligence and high-performance computing to address complex cyber challenges, leverage commercial providers, and maximize the use of the Software

Acquisition Pathway. Outdated hardware-centric acquisition processes hinder the delivery of cutting-edge technology to warfighters. Secretary Hegseth has therefore directed DoD to adapt to the reality of software-defined warfare by using the Software Acquisition Pathway as the gold standard for software development. This approach prioritizes rapid prototyping and scaling of solutions, leveraging commercial innovation to deliver minimum viable products in under a year. To further accelerate this shift, DoD will prioritize the use of Commercial Solutions Openings (CSOs) and Other Transaction (OT) authority for software acquisition, leveraging the agility of the commercial sector. This modernization effort extends beyond speed, emphasizing cybersecurity baked into the development pipeline and empowering those on the front lines with the tools they need to maintain a decisive edge in contested environments.

Conclusion

The dynamic nature of cyberspace and the rapid evolution of technology requires continuous adaptation and responsiveness to emerging challenges. DoD remains steadfast in its commitment to defending the Nation in cyberspace. This commitment extends to maintaining a Joint Force that is prepared to fight and win across the full spectrum of conflict, responding decisively to any threat to our national security.

We remain committed to exercising our full range of authorities to deter aggression, defend national security, and promote stability in cyberspace. The Department is deeply grateful for the ongoing support of Congress and looks forward to continued collaboration in addressing the complex challenges of the cyber domain. Thank you, and I look forward to answering your questions.