POSTURE STATEMENT OF

GENERAL JOSHUA M. RUDD, USA

COMMANDER, UNITED STATES CYBER COMMAND

BEFORE THE 119th CONGRESS

SENATE COMMITTEE ON ARMED SERVICES

28 APRIL 2026

(U) Chairman Wicker, Ranking Member Reed, and distinguished members of the committee, thank you for your support through my recent confirmation process and for the privilege of representing the men and women of U.S. Cyber Command (USCYBERCOM) and the Cyber Mission Force (CMF). I value our partnership and this opportunity to discuss the changing strategic landscape, the Command's accomplishments in 2025, and its way ahead in 2026. Last year the Command demonstrated its proficiency in integrating cyberspace operations with the Joint Force. This year, the Command continues to build upon our warfighting successes in defense of the nation, evidenced by on-going support to current operations.

(U) I've witnessed our critical role in integrating cyber operations across the Joint Force; including in South America, the Middle East, and the Indo-Pacific. We deliver and integrate capabilities that support Combatant Commanders while mitigating risk for the Department of War (DoW), and enhancing mastery in our cyber forces, all of which depend on our congressionally granted Service-like authorities, such as Joint Force Trainer, Enhanced Budget Control, and acquisition. These authorities allow USCYBERCOM to shape the force that the nation requires in cyberspace – and we are executing them as intended.

(U) OUR MISSION AND PARTNERS

(U) USCYBERCOM, through its subordinate unified commands and components, executes three assigned missions in support of the Department's and Administration's

priorities outlined in the National Security Strategy, the Cyber Strategy for America, and National Defense Strategy. The Cyber National Mission Force (CNMF) defends the nation from malicious cyberspace actors who threaten our homeland. The Department of War Cyber Defense Command (DCDC) operates, secures and defends the Department of War Information Networks (DoWIN) to ensure our warfighters can execute missions globally. Our Service-led Joint Force Headquarters-Cyber – JFHQ-C (Navy), JFHQ-C (Army), JFHQ-C (Marines), and JFHQ-C (Air Force) – enable full spectrum cyber operations in support of Combatant Commands' missions to meet the Department's priorities. Finally, I should also mention that Coast Guard Cyber, under the Department of Homeland Security (DHS) serves as a component of USCYBERCOM, bringing important capacity and authorities to support our operations. All our components enhance the effectiveness of our allies and partners, collaborating and enabling them to bear greater common defense burdens. Also, the recently published Cyber Strategy for America affords additional operational latitude for cyber to support national security objectives. This range of duties and activities demands effective coordination, robust intelligence, and a deep understanding of both the cyber domain and broader geopolitical contexts.

(U) I also serve as the Director of the National Security Agency (NSA), which is USCYBERCOM's closest partner. The Agency is simultaneously a Combat Support Agency, a key component of the Intelligence Community, and the security overseer for vital national security systems. NSA's roles, responsibilities, and capabilities complement those of USCYBERCOM. The synergy between these two organizations drives a unity of

effort and unity of Command that strengthens the Joint Force, the Intelligence Community, and ultimately the nation. With the dual-hat command relationship between USCYBERCOM and NSA, I can make and execute decisions at the speed of war and speed of relevance, contributing substantially to the nation's defense and the Department's ability to fulfill its mission.

(U) DEFENDING THE HOMELAND

(U) U.S. Cyber Command is in daily contact with malicious cyber actors, including state-sponsored entities working for our nation's adversaries. We have witnessed persistent efforts by state-sponsored cyber actors to achieve strategic objectives against the United States and its allies and partners. We see these actors probing the DoWIN, weapons systems, and critical infrastructure with the intent to hold our economic and national institutions at-risk. DoW systems and data – as well as critical civilian infrastructure in the United States – are being targeted, and our responsibility to defend them remains a no-fail mission for the Department and the nation.

(U) I am pleased to report that we are also increasing CMF talent, resources, and focus on behalf of the Combatant Commands directly engaged in defending the American homeland within their areas of responsibility and functional missions. To meet the demand, we continually reassess our force allocation and have realigned forces to ensure complete alignment with the National Security Strategy, the Cyber Strategy for America, and the National Defense Strategy.

(U) We are in direct support to U.S. Southern Command (USSOUTHCOM) in its operations with partners to counter foreign drug cartels, build meaningful partner capacity, and bring stability to the Western Hemisphere. This has entailed a wide range of cyberspace operations, including force protection, hardening DoW systems, hunt forward missions (more on these below), and integration across the full spectrum of military capability. In particular, I am proud of the proficiency and impact of USCYBERCOM's recent participation in Operation ABSOLUTE RESOLVE. Command personnel showed remarkable dedication, expertise, and sheer stamina in pivoting to integrate cyber effects and intelligence with USSOUTHCOM's mission in Venezuela.

(U) We support U.S. Northern Command (USNORTHCOM) in securing our borders. This means not only tracking and disrupting the supply chain that delivers fentanyl into America, but also assisting bilateral efforts against cartels that profit from the drug trade and human trafficking.

(U) We also support U.S. Strategic Command (USSTRATCOM), U.S. Space Command (USSPACECOM), and other DoW entities in bolstering defenses against attacks against the United States. USCYBERCOM, for example, is a key contributor to the President's Golden Dome for America initiative.

(U) Our efforts to defend the homeland flow through our Service components and the CNMF. CNMF personnel have deployed more than a hundred times in recent years to over 30 countries in partner-enabled missions to hunt on host networks. They conducted more than two dozen such "hunt forward" missions in 2025, generating insights and

constraining adversary freedom of maneuver around the globe. These missions frequently lead to public releases of malware samples for analysis by the global cybersecurity community. Such disclosures have made Internet users in America and around the world, as well as in host countries, safer on-line. They also frustrate the military and intelligence operations of authoritarian regimes.

(U) Our Command secures, defends, and operates the military systems and data that provide warning, situational awareness, synchronization, and sustainment for our fellow Combatant Commands. This work focuses on the defense of our warfighting networks. That is our supported mission at USCYBERCOM. Every Combatant Command's operational plan depends on the ability of leaders and commanders to communicate orders and share data securely.

(U) USCYBERCOM coordinates with Geographic Combatant Commands to identify key cyber 'terrain' to inform and prioritize DCDC and Service component's Defensive Cyber Operations (DCO) efforts. We seek to ensure our partners fully understand key mission systems and execute clearly defined roles and assignments for defending that terrain. When necessary, our Cyber Protection Teams work with local network defenders to secure and defend Joint Force systems, networks, and data.

(U) One of USCYBERCOM's primary sources of intelligence to identify and counter cyber threats such as ransomware attacks on U.S. critical infrastructure is FISA Section 702 collection. Intelligence derived from FISA Section 702 collection has proven invaluable in protecting our nation and warfighters overseas from terrorist attacks,

adversary state actors, and malicious cyber activity. I assess there is no substitute for the speed and reliability of FISA Section 702 collection, or the specific and actionable insights that FISA Section 702 collection yields in defense of the homeland and warfighter networks.

(U) USCYBERCOM is strengthening the network defenses of our warfighting networks in several ways. We are emplacing stronger, more dynamic cybersecurity measures; investing in artificial intelligence and machine learning to improve threat detection, response times, and predictive analysis; enhancing the knowledge, skills, and capabilities of our workforce; leveraging new and legacy authorities; and working with Allies, partners, and industry to make the DoWIN a more difficult target for our adversaries.

(U) Defending Joint Force systems and data parallels our efforts to support those who defend adjacent cyber terrain, particularly government, critical infrastructure, and partner networks. We work across the Joint Force and with a variety of partners to do this – something we call "Setting the Globe" – because systems in one region often depend on the functionality and the security of U.S. and foreign systems hundreds or even thousands of miles away.

(U) We collaborate with an array of U.S. and foreign partners to ensure that adversaries cannot impair that connectivity – or our decisionmakers' trust in its security. Foreign adversaries continuously sharpen how they operate, and frequently work through (unwitting) American-owned networks and systems. USCYBERCOM fosters unity of action across partners like the Service counterintelligence agencies, the Federal Bureau of

Investigation (FBI)-led National Counterintelligence Task Force, and DHS's Cybersecurity and Infrastructure Security Agency (CISA), sharing insights that enhance network defenses and counter adversary tactics. In addition, USCYBERCOM (with NSA) enables efforts by the Department of the Treasury, the FBI, and other partners to disrupt ransomware, cryptocurrency theft, and other criminal activities.

(U) Consistent with Congressional intent, USCYBERCOM engages in a two-way voluntary sharing of information with industry to help bolster private companies' ability to defend themselves against exploitation by malicious cyber actors and enhance our ability to act against those same actors. We aim to broaden the sharing of insights, ensuring mutual gain from this collaboration. Our UNDERADVISEMENT program, a voluntary collaboration with more than a hundred companies, links cybersecurity expertise across industry and government. This partnership has cued significant operational successes, enabling network owners to close vulnerabilities and eradicate threats from their systems. Such efforts by design frustrate adversaries and make their campaigns more expensive for them and less consequential for us.

(U) ENABLING DETERRENCE

(U) China seeks a world order more amenable to the Chinese Communist Party (CCP)'s vision and ideology – and views cyber as a critical domain for modern warfare. Not only is China confronting us in cyberspace, it is also expanding its sway in the Pacific while insisting that it is only acting to defend itself. China has constructed a substantial

cyberspace operations force, supported by capable and adaptive enablers in its native defense, cybersecurity, and information technology industries.

(U) Focusing on the strategic and operational challenges that China presents in cyberspace, our Command recognizes the vital role that we play in supporting the Joint Force in Pacific-area contingencies. We support U.S. Indo-Pacific Command (USINDOPACOM) in its mission to deter aggression and defend its area of responsibility. This commitment extends to the other Combatant Commands that would be involved in a Pacific crisis, particularly U.S. Transportation Command (USTRANSCOM), U.S. Special Operations Command (USSOCOM), and USSPACECOM. As noted, we also work daily with U.S. Government partners and industry to deny China-based cyber threats to our homeland, allies, and partners. We are countering China's cyber operators' efforts to burrow into U.S. critical infrastructure systems and pre-position for attack in a contingency or crisis scenario. We are also hardening DoW's cyber "terrain" across the Pacific region to make it more secure and defensible against any attacker. Our Command gratefully acknowledges the importance that our allies and partners provide in defending our common interests in the Pacific.

(U) We also support USINDOPACOM and U.S. Forces Korea in upholding deterrence on the Korean Peninsula. North Korea, like Iran, sponsors increasingly capable cyber actors. Pyongyang focuses cyber activities on the circumvention of international sanctions and the generation of illicit revenue through cryptocurrency exploitation that supports the regime's nuclear weapons and ballistic missile programs.

(U) We support U.S. European Command (USEUCOM) in stabilizing the security environment in Europe. Russia remains a threat to the peace of the Continent and to the global order. Moscow violates international norms with its aggression in Ukraine, coupled with its overt and covert campaigns to intimidate Ukraine's friends. As with China, Russia's military and intelligence cyber forces serve the Kremlin's strategic objectives – as we have seen time and again in the Ukraine war, the first major conflict with a full-fledged cyber front. Russian cyber actors work to subvert Ukraine and divide its Western allies, seeking to undermine them abroad and internally. In the Russian case, the Kremlin encourages, or at least tolerates, brazen cyber-criminal entities that indirectly serve state purposes against foreign targets.

(U) USCYBERCOM supports U.S. Central Command (USCENTCOM) and USSOCOM in their campaigns to counter Iranian aggression. With USCENTCOM, we have helped bolster the cyber defenses of Israel and other regional partners, including support for regional stability efforts. The Command has focused on securing key partners and networks in the region, and provides actionable information, insights, and options to policy makers.

(U) Non-state cyber actors remain a threat in cyberspace. Cyber criminals continue to find new victims in the United States and globally. We are concerned about the criminal enablers of such activities, such as those providing ransomware-as-a-service. In addition, violent extremist groups still spread propaganda and incite attacks in cyberspace. Though their capabilities have been eroded, the Islamic State in Iraq and Syria (ISIS), al Qaida, and

their offshoots maintain the intent to target Americans. Our Joint Force Headquarters-Cyber (Marines) works in conjunction with U.S. military and diplomatic efforts, supporting allies and partners who are disrupting terrorist messaging and mobilization online as well as providing critical intelligence.

(U) Strong partnerships with government, industry, academia, and foreign colleagues amplify our operational effectiveness and in turn create advantages for our partners. Such advantages force dilemmas upon our adversaries, and broaden the perspectives and insights we can utilize and exploit. Our components, when working in unison with diplomatic, military, law enforcement, homeland security, and intelligence capabilities, make a powerful combination that can disrupt the plans of malicious cyber actors wherever they hide. In addition, our Regional Cybersecurity and Engagement Strategy in the Indo-Pacific guides efforts with partners to counter and contest foreign adversaries. These efforts at USCYBERCOM go into fostering capacity building among partners, promoting interoperability, burden-sharing, and reducing barriers to information sharing and combined activities.

(U) USING OUR AUTHORITIES

(U) USCYBERCOM employs unique Service-like authorities to enhance readiness, improve capabilities, and advance partnerships. These authorities help to ensure that innovation adds speed, agility, and scale across operations, capability deployment, data sharing, and procurement.

(U) The Enhanced Budgetary Control (EBC) authority and resources granted by Congress are crucial to the execution of our Service-like functions. This portfolio of fiscal authorities has transformed our relations with DoW, the Services, and our Components. EBC entrusts nearly $4 billion of the DoW budget to USCYBERCOM, and streamlines how we engage the Department's planning, programing, budgeting, and execution processes. EBC also promotes the transparency that aligns authorities, responsibility, and accountability in cyberspace operations. Greater accountability in turn facilitates better cybersecurity as well as faster development and fielding of new capabilities.

(U) Agile acquisition is key to creating advantage for our commanders, components, and operators. The Command collaborates and partners closely with the Services, the Defense Advanced Research Projects Agency (DARPA), the Strategic Capabilities Office (SCO), Defense Innovation Unit (DIU), and others, to ensure our acquisition strategies enable agility, scale, and precision at the rapid pace demanded to keep the United States ahead of our adversaries in the cyber domain. For example, USCYBERCOM partners with DARPA through an acquisition initiative called CONSTELLATION to bridge the proverbial "valley of death" for new capabilities, which it can now transition more rapidly from concepts to operational use.

(U) Many of our missions depend on the Joint Cyber Warfighting Architecture (JCWA), a suite of systems with associated capabilities that facilitate a full range of cyberspace missions and foster overmatch against malicious adversaries. Our Command is employing its Department-approved systems engineering and integration authorities to

ensure JCWA develops efficiently in accord with a shared vision. Common standards between the Service-managed subcomponents of JCWA have accelerated its interoperability, tool development capacity, and data flows within and across the Command and mission partners. Finally, the Department is working with USCYBERCOM through our JCWA Program Executive Office (PEO) to provide our Command with milestone decision authority for the Service-managed JCWA programs of record.

(U) USCYBERCOM's designation as a federal laboratory for technology transfer empowered our work with industry and academia. Using our authorities as a federal lab, USCYBERCOM signs Cooperative Research and Development Agreements (CRADAs) with industry and academic partners. With thanks to Congress for amending this authority in the FY25 NDAA, we are now able to engage our territorial partners in such key areas as Guam. These agreements allow tighter collaboration between our operators and technical experts and, for example, local network defenders seeking to enhance their capabilities to detect whether their systems have been compromised. USCYBERCOM has also signed Education Partnership Agreements (EPAs) with a variety of institutions. Finally, our Academic Engagement Network (AEN) of more than 120 institutions is facilitating new partnerships and bringing fresh ideas to shared challenges.

(U) Artificial intelligence (AI) holds the potential to change the character of war. Automation and autonomy – in cases enabled by AI – are transforming ideas from theory into reality and even disruptive weapons and tools on battlefields and in competition

around the world. Our allies, partners, and adversaries are all engaged and propelling this technological progress. Adversaries employ AI for similar purposes as we do.

(U) Congress made a significant and strategic investment in our AI capabilities, and we are employing those resources effectively. USCYBERCOM's acquisition and programming authorities promote agile methodologies for rapid AI development and iteration, accelerating adaptation to evolving cyber threats and operational needs. The Command is implementing its framework for ensuring AI solution interoperability and integration across the cyber domain. This supports rapid prototyping, streamlined software acquisition, and the integration of commercial AI advances. USCYBERCOM is leveraging AI to enhance our capabilities in collection, detection, exploitation, maneuver, and command and control, generating greater speed and scale. A general officer in our headquarters is now leading our Command's effort to explore and apply artificial intelligence to the cyber mission set. He works with the AI Task Force in CNMF and already sees success in a growing series of pilot projects, many of which are having operational impacts today.

(U) In an environment transformed by AI and big data, operational and strategic advantage accrues to the side that sustains speed and efficiency in collecting and ingesting reams of data, building and employing models and algorithms, and deploying and updating them at-scale, while also denying similar advantages to adversaries seeking to exploit our systems and data. We are focused on ensuring our data and analytic infrastructures deliver advantage, and that those systems attain sufficient resilience to

function even under attack. Some of this work proceeds under the auspices of the DoW- and USCYBERCOM-developed five-year AI Roadmap. This guides the appropriate people, data, organizations, and infrastructure to deliver AI capabilities for all cyber mission sets; to counter AI threats and seize emerging opportunities; and to enable AI adoption.

(U) BUILDING AND SUSTAINING MASTERY

(U) I am pleased to report that all our Service cyber components and the forces they present to our Command remain mission ready, while consistently working to get better. This achievement rested on sustained efforts by the Services to improve the manning, training, and equipping of their respective forces. The staffing and training of our teams is improving, and the Command's cyber readiness system shares data directly with the Defense Readiness and Reporting System (DRRS). While our current force is meeting readiness standards, they are insufficiently scaled for the threat environment. The next year provides us a great opportunity to attack this problem.

(U) When the Department established USCYBERCOM in 2010 and authorized our Cyber Mission Force in 2012, it did not fully project the requirement to sustain cyberspace operations at-scale. The Assistant Secretary of War for Cyber Policy (ASW/CP), as the Department's Principal Cyber Advisor, is a key partner in meeting this challenge and has sharpened the Department's focus on cyber matters, which is instrumental to USCYBERCOM as we implement new authorities and evolve to increase domain mastery and warfighting readiness.

(U) With the ASW/CP, we are implementing our Revised Cyber Force Generation Model (commonly referred to as CYBERCOM 2.0). The Secretary of War recently endorsed several concepts to update USCYBERCOM's force generation and the ways in which we build and sustain specialization and expertise in our teams. Our revised model establishes policy, implements programs, and executes new approaches to recruiting, developing, and retaining cyber talent. In short, it will foster mastery across the force so we can overmatch quantity with quality. These steps were prompted and facilitated by Congressionally approved provisions on readiness and force generation that collectively gave the Department the opportunity to modernize the cyber force and reshape USCYBERCOM.

(U) CYBERCOM 2.0 calls for several new entities, which are currently under construction. These include a Cyber Talent Management Organization planned for the near year, followed by an Advanced Cyber Training and Education Center and a Cyber Innovation Warfare Center. These are slated to be operational in the near term. The Department and Command had the opportunity to explore these entities in a hearing before the Cybersecurity Subcommittee last month. Together they will help change the Department's approach to generating cyber forces, emphasizing domain mastery, strengthening specialized skills, and enhancing mission agility. Coupled with the readiness improvements highlighted above and organizational efforts to streamline the force, the end result will be a more experienced, better-trained, and better-equipped cyber force capable of adapting in the dynamic cyberspace environment. I look forward to

providing regular updates on the implementation of these initiatives to enhance lethality in the future.

(U) At USCYBERCOM, our Code is "We win with People." This principle guides a culture where initiative, innovation, collaboration, and the expertise of our personnel drive mission success. The people of USCYBERCOM are determined to defend our networks, counter threats, strengthen our partners, and provide decisive advantages for policymakers and military commanders. We amplify the impact of federal, military, foreign, and private-sector partner activities, synergizing the application of all instruments of national power against our adversaries. We seek to ensure our people have the necessary resources to optimize readiness and resilience.

(U) USCYBERCOM's efforts depend on the initiative, motivation, and excellence it sustains in its people. We must hire and retain critical expertise while ensuring all our personnel remain ready to meet the challenges of competition, crisis, and conflict in and through cyberspace. We are working to cultivate uniformed cyber leaders at all levels, up to and including the officers who will eventually succeed me in this post. Furthermore, USCYBERCOM's authorities as Joint Cyberspace Trainer facilitates joint training standards across the entire Department, boosting DoW's ability to defend networks while enabling CMF teams to focus on hunting and contesting foreign adversaries.

(U) The Department of the Army acts as our Combatant Command Support Agency. Army specialists are helping us fill our civilian billets and facilitating hiring actions to onboard exceptional civilians across the Command. We are leveraging the DoW Cyber

Excepted Service authority to streamline civilian hiring and offer competitive employment incentives. We also employ special hiring authorities offered in 10 U.S.C. 4092 to attract top technical talent to join USCYBERCOM, and look forward to hiring more experts in 2026.

(U) Finally, USCYBERCOM is exploring innovative ways to enhance our capabilities using the expertise resident in the National Guard and Reserves. Our personnel operate daily alongside activated members of the Reserve Component integrated into our teams, and we collaborate with National Guard units on State Active Duty and State Partnership Program engagements. We look forward to expanding ways to make the Reserve Component integral to our efforts. In particular, in a hearing before this committee on CYBERCOM 2.0, we noted options to improve USCYBERCOM's ability to leverage expertise in the Guard and Reserve, such as the establishment of a Joint Cyber Reserve Component or funded reimbursable authority.

(U) CONCLUSION

(U) U.S. Cyber Command creates advantage for the Joint Force, for the Department, for our partners at home and abroad, and for the nation. We operate in and through cyberspace to support national strategic goals and set conditions for the Joint Force to prevail in crisis and win our nation's wars. We must do so with greater agility and at a larger scale in 2026 because the United States and our allies face increasingly dangerous cyber threats from both state and non-state actors. We are meeting that need, and posturing our people and organization to accelerate their efforts. And we proceed with

scrupulous regard for the privacy and civil liberties of U.S. persons, and in an objective, non-partisan manner.

(U) Our operational experience at USCYBERCOM reinforces the central role of cyberspace in enhancing Joint Force combat credibility, lethality, and deterrence and contributing to overall national strategic objectives. The Command is executing its Service-like authorities to set and validate requirements, to plan and execute programs, and to administer budgets and resources. It is working with the Services to organize, train, and equip the nation's military cyber force, sustaining its readiness. USCYBERCOM's goal now is promoting mastery in our personnel by using the new resources and authorities Congress and the Executive Branch have provided. I am dedicated to creating a more lethal cyber force, operating with the speed, scale, agility, and precision required in the cyber strategic landscape.

(U) The warfighters at USCYBERCOM are grateful for the partnership with your Committee. I am proud and somewhat humbled that the President and the Congress have entrusted to me the duty of leading and representing our Service members and civilians, and I look forward to demonstrating how they are effectively managing their responsibilities, employing the resources that you have provided, and accomplishing our missions to defend our nation. With continued strong partnership with Congress, we will succeed. Thank you.