RECORD VERSION

STATEMENT BY

LTG PAUL M. NAKASONE

COMMANDING GENERAL U.S. ARMY CYBER COMMAND

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY

COMMITTEE ON ARMED SERVICES

UNITED STATES SENATE

FIRST SESSION, 115TH CONGRESS

U. S. ARMY CYBER POSTURE

MAY 23, 2017

NOT FOR PUBLICATION UNTIL RELEASED BY THE

COMMITTEE ON ARMED SERVICES

Introduction

Chairman Rounds, Ranking Member Nelson, and Members of the Subcommittee, thank you for your continued support of U.S. Army Cyber Command (ARCYBER) and our efforts to operationalize cyberspace for our Army. It is an honor to address this subcommittee on behalf of the dedicated Soldiers and Army Civilians of ARCYBER who work every day defending the Nation in cyberspace. This testimony focuses on ARCYBER's ongoing progress in the areas of Operations, Readiness, Resources, Training, and Partnering,

The Army Cyber Enterprise has made significant progress operationalizing cyberspace since my predecessor's testimony before the Subcommittee on Emerging Threats and Capabilities in April 2015. Since then, Army Cyber Command has completed the initial build of the Army's Cyber Mission Force (CMF). All 41 Active Component Army teams are at Initial Operational Capability or better and all are on track to be at Full Operational Capability by the end of September 2017, a year ahead of U.S. Cyber Command's (USCYBERCOM's) mandated timeline. The Army is now building an additional 21 Reserve Component (RC) Cyber Protections Teams (CPTs), trained to the same Joint standards as the Active Component teams, which will be integrated into the Army's Total Cyber Mission Force.

Additionally, the Cyber Center of Excellence (Cyber CoE) graduated its first class of Cyber Branch Lieutenants in May 2016; its first class of Cyber Warrant Officers in March 2017; and began training its first class of new cyber enlisted recruits also in March 2017. The Cyber CoE trained a total of 582 Cyber Branch Soldiers during Fiscal Year (FY) 2016 and is scheduled to train another 1,200 Soldiers during FY2017. The Army cyber force now includes 2,331 Soldiers with career fields that include Cyberspace and Electronic Warfare operations. (557 Officers, 305 Warrant Officers, and 1,469 Enlisted). Furthermore, the Cyber Center of Excellence recently published Field Manual (FM) 3-12, Cyberspace and Electronic Warfare Operations, which provides overarching doctrinal guidance and direction to the Army for conducting cyberspace and electronic warfare (EW) operations in unified land operations. Army Cyber Command is continuing its Cyber Electromagnetic Activity (CEMA) Support to Corps and Below pilot program and is now working with our Army partners to determine

enduring support requirements at the combat training centers and ultimately, cyber force structure and requirements at the tactical level within the Army.

The Army also recently made several important organizational changes to the Army Cyber Enterprise to improve our ability to conduct cyberspace operations and support Joint and Army commanders. First, the Army elevated ARCYBER to an Army Service Component Command (ASCC) ensuring ARCYBER receives the same level of resourcing as other ASCCs supporting Combatant Commanders. Second, the Army reassigned the Network Enterprise Technology Command to ARCYBER to better align responsibilities and authorities to support USCYBERCOM and Army requirements and to better align roles and responsibilities for the Army's portion of Department of Defense Information Network (DoDIN). Third, the Army established an Army Cyber Directorate within the Headquarters Department of the Army (DAMO-CY), to advocate and coordinate cyberspace doctrine, policy, organization, and resourcing issues within the Pentagon. The DAMO-CY Directorate joins the Army's Cyberspace Tetrad that includes the Army Cyber Institute, the Cyber Center of Excellence, and ARCYBER. Finally, the Army broke ground for the new Army Cyber Headquarters Complex at Fort Gordon, Georgia in November 2016, and has committed to future investments in new Cyber Center of Excellence facilities in which to train our Soldiers.

Army Cyber Command is building on the Army's past progress while focusing on three key priorities: Aggressively Operating and Defending Our Networks, Data, and Weapons Systems; Delivering Effects Against Our Adversaries; and Designing, Building and Delivering Integrated Capabilities for the Future Fight. Today, Army cyberspace forces, including Reserve Component forces, are improving the Army's cybersecurity posture; protecting and defending Army and DoD networks, systems, and critical infrastructure; supporting Joint and Army commanders; and engaging our adversaries in cyberspace every day.

While ARCYBER has made significant advances building the Army's cyberspace capacity and capabilities over the past six years, our progress will be overshadowed by the inability to maintain overmatch against near-peer competitors due to a lack of sustained, long-term, and predictable funding. As evidenced by the recent threat of a year-long continuing resolution, the Army would have been forced to stop funding for

Army National Guard Cyber Protection Teams. This would have slowed the Army's ability to fulfill the congressional mandate to integrate Army Reserve Component Cyber Protection Teams into the Cyber Mission Force. The Continuing Resolution delayed the fielding of the Joint Persistent Cyber Training Environment leading to greater costs and delays in building DoD cyber capability and capacity. Further, a major impediment to improving Army cybersecurity through network modernization has been a lack of predictable funding. The Army needs an end to the year-after-year continuing resolutions and relief from the Budget Control Act of 2011 to help restore readiness levels and build force capacity and capabilities to counter emerging threats, including those in cyberspace.

Operations

Cyberspace operations encompass three interrelated areas: Department of Defense Information Network (DoDIN) operations, Defensive Cyberspace Operations (DCO), and Offensive Cyberspace Operations (OCO). Army DoDIN operations are the most complex, most important mission ARCYBER conducts. They include building, operating, defending, and maintaining the Army's portion of the DoDIN. Our five Regional Cyber Centers conduct DoDIN operations around-the-clock, serving as the Army's Cybersecurity Service Providers (CSSP). The Army continues to work with U.S. Strategic Command and the Joint Chiefs of Staff to realign our DoDIN force structure in accordance with the 2017 NDAA and to gain better command and control over the global cyber theater.

To support DoDIN operations and improve cybersecurity, the Army is building a more reliable, secure and ready network through system hardening and modernization. A new effort between ARCYBER and the Army's Chief Information Officer/G6 (CIO/G-6), called the "DoDIN Initiatives" is key to our system hardening efforts. This initiative focuses on information sharing to include tracking progress, identifying gaps and issues with policies or resources to unify the way ahead for the Army.

The greatest challenge and most critical aspect of a ready, secure, and available network is a modern and resilient infrastructure. In the Army we refer to our efforts to achieve this as Network Modernization (NETMOD). The Army's NETMOD efforts

include: Joint Regional Security Stack (JRSS) migration, Multiprotocol Label Switching upgrades, and Installation Campus Area Network upgrades. The Army is partnering with the U.S. Air Force and the Defense Information Systems Agency (DISA) in deploying JRSS to centralize the Army's existing perimeter security infrastructure. The Army has completed the upgrade of 22 of its installation's network infrastructure and migrated them to the JRSS. The Army continues to upgrade its installation's network infrastructure and migrate within the JRSS. The current plan is a phased approach upgrading installations within CONUS, Southwest Asia and European Theater, followed by the Pacific Theater, to include Korea and Alaska, with main installations being complete by fourth quarter FY 2019. At the next layer of Network Modernization, DISA has completed upgrading the Army's fiber optics and Multiprotocol Label Switching circuits of 18 installations and is focused on completing seven more sites this year. These initiatives, in combination with the increased capabilities of our operational force, will enable stronger cyber protection, detection, and response to cyber threats across the DoDIN.

In order to take advantage of these DoD network improvements at the Army Base/Post/Camp/Station level, we must modernize our own infrastructure through Installation Campus Area Network upgrades. This is an enduring effort to stay current with technological advances. A top DoD and Army priority, aimed at hardening our endpoints and infrastructure, is the implementation of assuring appropriate upgrades to our operating system and applications. The DoD-managed common secure host baseline will allow the Army to strengthen our cybersecurity posture while concurrently streamlining the IT operating environment. Additional end-point efforts include one focused on security and one on management. All these efforts combined enable us to provide the Army with a ready, secure, and available network that supports Mission Command and supports the projection of combat power. While the Army's investment in network hardening and modernization has paid dividends, ARCYBER would benefit from predictable funding for DoDIN operations. A lack of predictable funding is the major impediment to improving Army cybersecurity through network hardening and modernization.

In addition to building a more defendable network, ARCYBER conducts both passive and active Defensive Cyberspace Operations to protect and defend the Army portion of the DoDIN. Defensive Cyberspace operations are mission focused, prioritized on critical assets, and threat specific. Our Cyber Protection Brigade, (CPB) and its Cyber Protection Teams, conduct critical active defense of the DoDIN. The CPB's ability to conduct active recon for advanced persistent threats distinguishes them from the functions of a CSSP that is dedicated to protecting our network against known threats. Our CPTs are a maneuver element in cyberspace that reinforce the protection mission of a CSSP based on analysis of the mission relevant cyber terrain and threats provided by national intelligence and our own internally-collected cyber intelligence. The CPB also helps protect and defend the Army's critical infrastructure and support both national requirements and Joint and Army commanders around the globe. The Brigade includes 900 Soldiers and Civilians who make up 20 Active Component Cyber Protection Teams.

Importantly, our Cyber Protection Brigade supports Army Mission Assurance, providing Critical Infrastructure Risk Management assessments to identify potential vulnerabilities and threats. The CPB works with Department of the Army, Army Material Command, U.S. Army Corps of Engineers (USACE), and other stakeholders in an Army-wide approach to ensuring the cybersecurity of critical Army systems and infrastructure, including the Nation-wide systems of dams and hydroelectric plants USACE manages. Our CPTs deploy worldwide (including austere environments) with mobile capabilities within hours of notification, employing platforms and tools across the breadth and depth of our network. Our teams also provide "reach-back" support to deployed forces that allows us to put the right person on the right task at the right time.

The pace of operations and dynamic nature of the threats means our cyberspace forces engage with our adversaries in cyberspace as they are being built, usually before they achieve full operational capability. Both defensive and offensive Army cyber forces are rapidly maturing and building credibility with our combatant commanders in warfighting operations every day; continually learning and innovating their tactics, techniques, and procedures against determined, adaptive and aggressive adversaries.

Our Army Cyber Mission Forces execute Offensive Cyberspace Operations, to

project power by the application of force in or through cyberspace, under the authorities of Combatant Commanders and USCYBERCOM. Established by USCYBERCOM in June 2016 and commanded by the ARCYBER Commander, JTF-ARES is a Joint cyber operational headquarters providing cyber capabilities in support of US Central Command's counter-ISIS operations. The Task Force has brought cyber out of the shadows and successfully demonstrated the value and capabilities of cyberspace operations to the Joint Force when integrated as part of broader coordinated military effort.

Readiness

Readiness is the Army's overriding priority. To support readiness, the Army is building 62 Total Force CMF teams, all trained to the same joint standards, to support Joint and Army commanders. The 41 Active Component (AC) teams are built and conducting cyberspace operations supporting real world operations today. They are also defending DOD networks, protecting Army weapons systems, and defending critical infrastructure. Currently, 33 of the Army's 41 AC teams are at full operational capability, while eight teams remain at initial operating capability. By 30 September 2017, all 41 teams will be fully operational. With the completion of the CMF build, the Army is now progressing from building its cyber force to measuring the readiness of this force. Army Cyber Command is working with USCYBERCOM to implement metrics to measure CMF readiness through the Defense Readiness Reporting System.

Reserve Component Cyber Protection Teams

The Army's Reserve Component (RC), comprised of the Army National Guard (ARNG) and U.S. Army Reserve (USAR), is critical to Army readiness. The RC is building 21 Cyber Protection Teams (11 ARNG, 10 USAR) creating a Total Force solution, all trained to the same Joint standards as the Active Component. As required under Section 1651 of the National Defense Authorization Act of Fiscal Year 2017, the Army is implementing a Total Army RC cyber strategy to integrate the 21 RC CPTs into the Army's Cyber Mission Force to support Joint and Army cyberspace requirements.

Network Readiness

Network readiness is a component of Army readiness. Today the Army and the Joint Force depend on unimpeded access to the DoDIN for everything from business operations to missile defense. The network is now not only a critical enabler, but also an operational capability for cyberspace operations, vital to our operational readiness, and therefore important to measure. The Army currently measures network compliance with policy, regulation, and law through the Cybersecurity Scorecard, Command Cyber Readiness Inspections, and Command Cyber Operational Readiness Inspections.

Army Cyber Command partnered with JFHQ-DoDIN to execute the next evolution of Cybersecurity inspections under the Command Cybersecurity Operational Readiness Inspection (CCORI), to replace the Command Cyber Readiness Inspection. The CCORI moves cybersecurity inspections from a compliance-based systems inspection to a risk-based Operational Commander's Mission focused inspection. The CCORI highlights the risks to operational missions within a Command by employing active external and internal threat actors against a Commander's mission critical systems. The CCORI outcome provides an operational risk measurement to mission by mission critical task and a system to assist Commanders in prioritizing cybersecurity resources.

The DoD Cybersecurity Scorecard has brought basic cybersecurity hygiene to the forefront at the DoD level and has forced the Army to prioritize basic cybersecurity requirements. The Army has made strides towards remediating identified critical vulnerabilities across the enterprise and capturing the effectiveness of remediation efforts. The Army continues to work with DoD CIO to refine the Scorecard metrics to move from cybersecurity compliance to risk-based scorecard measurements to provide a mission assurance focus.

Training

Army Cyber Mission Force training has three key components: individual, collective, and mission rehearsal. Individual training is focused on formal training, work role specific training, and job-specific qualification and certification training conducted at

the work center. Individual training focuses on building individual core competencies, proficiencies, skills and knowledge necessary to accomplish assigned tasks.

During collective training, team members train in realistic environments and to relevant threats. Army CMF teams will conduct approximately 80 collective training events, throughout FY2017 to ensure they are fully trained to USCYBERCOM joint standards. Live, virtual, and constructive scenarios are used to ensure that training is holistic, repeatable, and measureable. Collective training is used to increase team proficiency, certify teams for operations, and allow leaders to build trust and confidence within their teams. Participation in USCYBERCOM exercises, CYBER GUARD and CYBER FLAG, helps achieve certification or revalidation.

Mission rehearsal training events are conducted to ensure that leaders understand their missions, the threats and risks they will face, and are prepared for contingencies. Army CMF teams are scheduled to conduct 48 internal mission rehearsal type training events during FY17 in order to build team proficiency, preparation for recertification/revalidation and mission preparations to support operations. These events occur at home station, training centers, and in deployed areas. Army Cyber Command teams also participate with Joint, interagency and coalition partners through Combatant Command training exercises for operational mission sets.

The Cyber Center of Excellence (CCoE) located at Fort Gordon, Georgia, operates the Army's Cyber School and trains Army Cyber Branch Soldiers and members of the other Services. All three cohorts, officer, warrant officer and enlisted, conclude their training by participating in Joint exercises ensuring they are well prepared to support Army units at all levels.

The CCoE is explicitly charged with incorporating Joint standards into the curriculum. The Joint Cyber Training and Certification Standards set work roles and training to a single joint standard applied across multiple Services building like teams. It unites the Services' efforts to train and certify their respective CMFs to perform in a joint environment. The CCoE focuses on individual training and has begun training key USCYBERCOM J7 pipeline courses including Cyber Common Technical Core (equivalent to Intermediate Cyber Core), CPT Core Methodologies, Cyber Operations Planner Course, and the Joint Advanced Cyber Warfare Course. Since the Army

established the Army Cyber Branch, Career Field 17 in September 2014, the CCoE has trained 1,500 Cyber Branch Soldiers. Fiscal Year 2018 will see more Soldiers trained in the Army 17-series pipeline, and Soldiers will continue to attend Military Occupation Specialty qualification courses. Graduates of these courses will provide a steady stream of trained 17-series Soldiers, thus decreasing the individual training burden on units and improving force readiness.

Establishing a Persistent Cyber Training Environment (PCTE) is central to training the Joint Cyber Mission Force and maintaining high levels of proficiency. In support of section 1645 of the FY16 National Defense Authorization Act, DoD designated the Army as the acquisition authority for the PCTE. The PCTE will provide high quality scenarios and event management for individual, team/collective, and mission rehearsal training for all four Services and USCYBERCOM. At maturity, we envision the DoD Joint PCTE platform as a constellation of federated, interoperable common training capabilities—enabling training from individual competencies at the team, unit, group and force training levels; including exercises, tactics, techniques, and procedures development, up to mission rehearsal.

CEMA Support to Corps and Below

In 2015 the Army initiated a Cyber Electromagnetic Activities (CEMA) Support to Corps and Below (CSCB) pilot program. The CSCB effort serves four primary purposes: Define what offensive and defensive cyber effects to integrate at the echelon Corps and below; Determine expeditionary Defensive Cyberspace Operations, Offensive Cyberspace Operations, Electronic Warfare, and Information Operations capability for deployed tactical forces; Leverage Combat Training Centers (CTCs) and operational deployments to inform CEMA Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities development (DOTMLPF); and Determine the enduring CEMA environment at CTCs.

Army Cyber Command recently completed its sixth iteration of the CSCB pilot and will conduct another one in June 2017. Lessons learned from the pilot program are helping to inform CEMA requirements across the Army's DOTMLPF and Policy development. Army Cyber Command is now working with DAMO-CY to determine

enduring support requirements at the CTCs that would routinely embed cyber teams in combat brigades during their CTC rotations to continue providing realistic training for our cyber operators, Army units, and commanders.

The Cyber Center of Excellence published the Army's first Cyberspace and Electronic Warfare doctrine in April 2017, FM 3-12, Cyberspace and Electronic Warfare Operations. Army FM 3-12 is nested in joint cyberspace and EW doctrine and provides the doctrinal context to understand the fundamentals of integrating and synchronizing cyberspace and EW operations. Through the planning and synchronization of cyberspace and EW operations, Army cyberspace forces integrate CEMA functions and capabilities across warfighting functions, defend the network, and provide critical capabilities for commanders at all levels during unified land operations.

Resources

People are the most important resource in cyberspace. To ensure we will prevail over all adversaries in the cyber domain, the Army is committed to executing a vigorous cyber talent management program built on four talent management pillars: recruit, develop, employ, and retain talent. The Army achieved a major milestone in cyber talent management in 2014 when it became the first service to launch a dedicated career field (Career Field 17) to centrally manage Soldiers throughout a career in cyberspace operations. This allows the Army to recruit, develop, employ and retain Soldiers specific to cyber skills and operations.

To ensure we continue to maintain high levels of end strength in the cyberspace force, the Army is now implementing several key talent management initiatives to improve recruitment, training, and retention across all components and all Soldier and employee cohorts. First, the Army is developing a direct commissioning program to find highly talented individuals with industry experience and laterally enter them into the force. Second, the Army has initiated a Civilian Cyber-effects Career program. Additionally, ARCYBER is offering opportunities to many members of our force, including the chance to train with industry and opportunities for academic degrees through our Advanced Civil Schooling program. Finally, we are partnering with the U.S.

Digital Service and the Defense Digital Service to help us look internally at our processes and provide an outside perspective from a group of technical experts.

The Army direct commissioning program, authorized under section 509 of the National Defense Authorization Act for Fiscal Year 2017, will bring in talented individuals with highly technical skills at ranks of increased pay and responsibility. The Army hopes to attract individuals with skills that include computer programming, mathematics, network operations, cryptology, data science, or nanotechnology. Beyond technical knowledge, we're looking for people with aptitude, dedication, and desire for mission- and team-oriented problem solving.

The Army recently approved the new Civilian Cyberspace-effects Career Program which will unify all Cyberspace Effects civilian employees into a single cross-disciplinary model for training and management of multiple Occupational Specialties This new career program will align Army Civilians performing Cyberspace Effects with their Soldier counterparts in Cyber (17 series). The Cyberspace Effects work role qualifications will be governed by USCYBERCOM Joint training requirements. The Department of Defense is also finalizing work on a new Title 10 excepted service civilian cyber program similar to the civilian intelligence career program.

Integration of Electronic Warfare

To better manage its Electronic Warfare Soldiers, in 2014, the Army approved the integration of cyber effects and electromagnetic spectrum operations into the Army's new Cyber Branch. The Army Cyber Center of Excellence is developing a phased approach to convert Soldiers in the Army Electronic Warfare Military Occupational Specialty, Functional Area 29, into the Cyber Branch beginning in FY2018. Concurrently, the Army is analyzing and developing an integrated Electronic Warfare, Cyber, and Signals Intelligence capability that will be capable of sensing and disrupting adversary systems that operate within the electromagnetic spectrum while providing Electronic Protection to Army systems.

Equipping the CMF

Army Cyber Command is focused on equipping the Cyber Mission force with integrated capabilities and organic development environments. To ensure that our capabilities are dynamic and evolving to counter future threats we are focusing on two mission areas of development: Defensive Cyberspace Operations and Offensive Cyberspace Operations. These two areas include the development of a scalable Big Data platform, building advanced cyber analytics, development operations support for payload development, malware analysis, threat detection, and infrastructure.

The Army has also invested in developing home station and deployable platforms that will provide our Defensive Cyber Operations CPTs with systems to support the defensive force with tools to prevent, mitigate, and recover systems at risk from cyber threats at near real-time speed. We are sprinting to build and institute a complete OCO architecture purpose built to enable operational agility, reduce training complexity, and maximize our ability to present multiple dilemmas to our adversaries. This effort includes the integrated build of a tool developer environment, operational infrastructures and foundational tools that support current and future mission requirements for the Army's Total Cyber Mission Force.

Road to Fort Gordon, Georgia

Army Cyber Command Headquarters is currently split-based at Fort Belvoir, Virginia, Fort Meade, Maryland, and Fort Gordon, Georgia, in overcrowded and inadequate facilities. The Army has begun building a $180 million, state-of-the-art Army Cyber Headquarters Complex alongside National Security Agency-Georgia at Fort Gordon, Georgia. Occupation of the new facility is planned to begin in 2020 with the full transition of ARCYBER Headquarters to Fort Gordon expected no later than 2022. The colocation of these operational forces with the Cyber Center of Excellence at Fort Gordon, will create significant synergy, allowing for the immediate incorporation of lessons learned and operational knowledge into our training curriculum.

Partnering

Partnerships are crucial to staying ahead of our adversaries in cyberspace. The Army Cyber Enterprise partners with industry, academia, the intelligence community, and our interagency partners to share information and find solutions to cybersecurity challenges. The Army is also adapting its acquisitions systems and reaching out to smaller “non-traditional” companies on the cutting edge of technology to keep pace with cyber threats.

To better leverage private sector and academic partnerships the Army has undertaken initiatives under DoD umbrella programs such as Defense Innovation Unit Experimental, or DIUX, the Defense Digital Service, and “Hacking 4 Defense” efforts to further reach-out and collaborate with non-traditional partners. Through DIUX, Active and Reserve Soldiers collaborate with private industry in Silicon Valley to quickly leverage commercial innovations into acquisition solutions.

During November-December 2016, working with a private sector partner, the Army launched the "Hack the Army" initiative, to crowdsource cyber vulnerabilities of selected Army Websites and databases. The Army paid a modest “bug bounty” to selected ethical hackers which helped the Army discover dozens of vulnerabilities. Army Cyber Command subsequently shared these vulnerabilities with the Intelligence Community.

To help foster innovation and partnerships between the Army Cyber Enterprise and the greater cybersecurity community, the Army Cyber Institute (ACI) at West Point serves as the Army's bridge to academia, government, and the private sector. The ACI facilitates state, local, public, and private partnerships in the cyber domain across the United States and Internationally. The ACI creates relationships that build capacity within major metropolitan centers and through exercises designed to integrate all levels of national cyber response. For example, in October 2016, ACI partnered with the NATO Cooperative Cyber Defence Centre of Excellence to develop a robust international conference on cyber conflict that will be repeated in November 2017.

In all partnering activities, the Army Cyber Enterprise is preparing for a future that includes machine learning, intelligent systems, virtual/augmented reality, and Big Data; in conjunction with ubiquitous computing, autonomous, and semi-autonomous robotic systems. The Army's partnering activities help prepare forces that bridge the military-civilian and peacetime-wartime boundaries needed to deal with the gray space nature of cyber conflict.

Conclusion

The Army has made significant progress operationalizing cyberspace since it established Army Cyber Command a little more than six and a half years ago. The Army now has 41 Cyber Mission Force teams and is building an additional 21 RC teams. The Army also has a Cyber Branch to support Cyber Soldiers throughout their careers and will soon have a Civilian Cyberspace Effects Career Program, tailored to our unique mission. The CyberCoE is training Cyber Soldiers and preparing to integrate the Electronic Warfare force into the cyber career field. We have broken ground on the Army Cyber Headquarters Complex on Fort Gordon, Georgia which will transform the Fort Gordon region into a cyberspace hub for the Army and the Nation. And the Army has also implemented important organizational changes to the Army Cyber Enterprise that enhance our ability to conduct cyberspace operations and support Combatant and Army commanders. These accomplishments have happened because the Army, with the support of Congress, has made protecting and defending the Nation in cyberspace a priority.

Our investments in the Soldiers and Civilians who carry out our critical mission are paying off. Today our teams are actively protecting and defending Army and DoD networks; securing Army weapons platforms; protecting critical infrastructure; and conducting operations against global cyber threats. These teams are delivering effects against our adversaries, giving our ground commanders and the Joint force the competitive advantage they need to win. With the continued support of Congress, the Army will maintain its tremendous momentum in cyberspace, building a more capable, modern, ready force that is prepared to meet any adversary in cyberspace, today and tomorrow.