PRESENTATION TO THE
SENATE ARMED SERVICES COMMITTEE
SUBCOMMITTEE ON CYBERSECURITY
UNITED STATES SENATE

SUBJECT: Military Cyber Programs and Posture

STATEMENT OF: Major General Chris P. Weggeman
Commander, 24th Air Force and
Commander, Air Forces Cyber

May 23, 2017

Introduction

Chairman Rounds, Ranking Member Nelson, and distinguished members of the Subcommittee, thank you for the opportunity to appear before you today, along with Vice Admiral Marshall Lytle from the Joint Staff and my fellow Service Cyber Component Commanders. I look forward to discussing the Air Force's progress in advancing full-spectrum cyberspace operations and our contributions to joint operations globally. I have the distinct honor to lead a triple-hatted organization; 24th Air Force, Air Forces Cyber (AFCYBER), and Joint Forces Headquarters (JFHQ) – Cyber AFCYBER. These three-hats encompass service, component, and functional roles, responsibilities, and authorities which I will expand upon shortly. Our headquarters is located at Joint Base San Antonio-Lackland, Texas and we have Airmen and civilians on-mission around the world, diligently increasing our capability to deliver full spectrum cyber effects in support of our joint warfighters.

AFCYBER warriors are operating globally as a maneuver and effects force in a contested domain, delivering cyber superiority for our Service and our joint partners. Our forces exist to preserve our freedom of maneuver in, through, and from cyberspace while denying our adversaries the same. Our Command places significant emphasis on operationalizing cyberspace as a warfighting domain across the range of military operations and continues to evolve our tradecraft to provide ready cyber forces to Combatant and Air Force Commanders across the globe.

As Commander, 24th Air Force, I report directly to the Commander of Air Force Space Command and am responsible within the Air Force for classic Title 10 organize, train, and equip functions. 24th Air Force also serves as the Cyber Security Service Provider (CSSP) for our Air Force networks and other designated key cyber terrain. Under the AFCYBER hat, I am the Air Force's Cyber Component Commander who presents and employs Air Force cyber forces to United States Strategic Command, delegated to United States Cyber Command. These ready forces plan and execute full-spectrum cyberspace operations across the Air Force portions of the DoD Information Network (DoDIN), and other cyber key-terrain as directed. Finally, under my third hat, as Commander, Joint Forces Headquarters (JFHQ) – Cyber AFCYBER, I lead a United States Cyber Command subordinate headquarters with delegated Operational Control

of assigned cyber combat mission forces employed in a general support role to both United States Strategic Command and United States European Command. We execute assigned cyberspace operations missions through six distinct but inter-related lines of effort—Build, Operate, Secure, Defend, Extend, and Engage, or what we refer to as "BOSDEE".

DEFENSE is our #1 Mission

In our 24th Air Force and AFCYBER roles, we build, operate, secure, and defend the Air Force networks every day to ensure these networks remain available and secure for assigned missions, functions, and tasks. The broader mission includes base infrastructure, business, and logistics systems, as well as mission and weapon systems; in total, providing on-demand capabilities to approximately one million users worldwide. The Air Force CIO designated 24th Air Force as the CSSP for all systems within the Air Force enterprise. In this capacity we are responsible for protecting, monitoring, analyzing, detecting, and responding to malicious cyber activity across the Air Force network. We are working with our Service Staff and Air Force Space Command, to determine resource and manpower requirements to execute this expansive mission-set. Earlier this year, we partnered with the United States Army Research Lab to contract and provide a fee-for-service cyber security framework for system cybersecurity similar to what they are providing the United States Army. This partnership and approach aligns the Air Force CIO delegated cybersecurity responsibilities with our AFCYBER defensive mission forces and capabilities, generating coherent mission coordination and integration across the enterprise.

Cyber Security and Defense in the 21st Century

24th Air Force, in collaboration with our Service staff and Major Commands, developed and began implementation of three transformational efforts which transition our force and Information Technology posture towards a 21st century, Commander and cyberspace operator driven, threat and risk-based mission assurance cyber ecosystem. These three major efforts include; 1) evolving towards the Air Force Information Dominance Platform (AFIDP), 2) maturing and resourcing our Air Force CIO Cyber Squadron Initiative and inherent Mission Defense Teams, and finally 3) the development and fielding of Air Force Material Command's Cyber Resiliency of

Weapons Systems (CROWS) Office capabilities. This last initiative was developed to address last year's NDAA Section 1647 weapon system cyber security mandate. These three major endeavors, deliver a coherent approach to cyber security, cyber defense, weapon system resiliency, and the ever critical "every Airmen a sentry" cyber hygiene culture across our Air Force.

The AFIDP is a network reference architecture designed to smartly divest the costly and manpower intensive network operations, maintenance, and customer-service support demands of our Service's dated, Information Technology infrastructure via outsourcing to commercial and industry partners. This strategy allows us to improve our network while repurposing portions of our legacy Information Technology workforce to deliver essential services, data security, and cyber-based mission assurance. The AFIDP moves the Air Force towards a risk-managed, Network and/or Infrastructure as a Service model (NaaS/IaaS). AFIDP, with Cloud Hosted Enterprise Services, which is currently in operation under the moniker "Collaboration Pathfinder", is securely hosting over 60,000 user accounts across ten bases. This service delivery model will enable improved network performance, reliability and scalability. It also fuels superior cyber security and defense, while generating superior speed, agility and precision of maneuver in, through, and from cyberspace.

The AFIDP roadmap leverages on-going Joint Information Environment (JIE), Joint Regional Security Stack (JRSS) migrations and fielding in close partnership with the United States Army and the Defense Information Services Agency (DISA). All DoD components will ultimately utilize JRRS with the United States Air Force and Army currently undergoing migration. Combatant commands, Coast Guard, and other Defense Agencies are scheduled to begin JRRS migrations later in FY17 and into FY18. To date we have successfully migrated two CONUS regions, to include 170,334 users across 32 bases. JRSS provides state of the art security stacks and capabilities at our Tier-2 gateway boundaries. AFIDP also employs the Automated Remediation and Asset Discovery (ARAD) capability suite.

ARAD is an instantiation of the commercial Tanium product, enabling operators to perform vulnerability management, incident response, system health diagnostics, as well as asset identification and optimization in a matter of seconds to minutes vice days

to weeks using current capabilities. ARAD achieved Initial Operational Capability on the Air Force Network in December 2016, installed on nearly 600,000 end-points with powerful results and exceeding all expectations. The ARAD team drove an unprecedented eight-month acquisition schedule to deliver tools that enable operators to identify and fix network vulnerabilities in seconds instead of weeks, and it provides the ability to detect, track, target, engage, and mitigate adversarial activities in near real time. The 24th Air Force ARAD team was awarded the 2016 Department of Defense Chief Information Officer Award for Cyber and Information Technology Excellence for their pioneering innovation. The demonstrated potential of ARAD is truly revolutionary, and we are diligently experimenting, evolving, and developing operational concepts and applications to close key mission capability gaps in close partnership with the Tanium experts. The intrinsic operational value and potential of ARAD/Tanium was formally acknowledge by the Air Force CIO, Lieutenant General William Bender, who recently directed ARAD implementation across the Air Force network to include mission systems and enclaves.

The second transformational effort is the Air Force Cyber Squadron Initiative (CSI). It is centered on an active cyber defense model across all echelons of Air Force organizations, designed to deliver enterprise mission assurance in a contested domain, in the presence of a maneuvering adversary. Cyber Mission Defense Teams (MDTs), the primary unit of action, are tailored, trained, equipped and task-organized to survey, secure, and protect key cyber terrain in order to deliver mission assurance. The Cyber Squadron Initiative is a Commander and mission-driven force employment model. Mission Defense Teams employ a spectrum of cyber security and defense tactics, techniques, and procedures in addition to their own suite of tailored cyber defense sensors and tools to provide active defense at the base level. In FY16 the Air Force executed fifteen Mission Defense Team “pathfinder” initiatives across a diverse set of Air Force missions and organizations to test and validate the operational concept and tool requirements. These designated units focused on functional mission analysis, planning, and network characterization. FY17 programming designates another fifteen Service-funded initiatives, as well as sixteen Major Command-funded initiatives. Although the Mission Defense Team concept is a nascent cyberspace defense

capability, these teams are already proving their worth; providing mission assurance for operational commanders' priority missions and mission systems. Laying the foundation, the 50th Space Communications Squadron's Mission Defense Team provided the Wing Commander with an understanding of cyber risk being accepted on the Air Force Space Control Network. The 52nd Communication Squadron Mission Defense Team integrated with AFCYBER Cyber Protection Teams to resolve a Combat Air Force cyber incident, defending Commander's key cyber terrain and allowing Wing Commanders to understand the operational risk if cyber hygiene is not a priority.

The third transformational effort is Air Force Materiel Command's Cyber Resiliency of Weapons Systems, or CROWS office. Their mission is to increase cyber resiliency of Air Force weapon systems across our acquisition and life cycle management processes to maintain mission effective capability under adverse conditions. CROWS have two primary objectives; first, to "bake-in" cybersecurity into developmental and future mission and weapons systems, and second; to employ a prioritized threat- and risk-based, cyber vulnerability assessment of existing systems to best mitigate risk to missions and forces. Their roadmap to cyber resiliency advances from systems assurance to the institutionalization of cyber security, cyber hygiene, and resiliency across all Air Force weapons systems. Their comprehensive strategy includes sustainable and programmable tools, infrastructure, and a skilled cyber workforce of operators, system engineers, and acquisition professionals to deliver end-to-end mission and weapon system cyber security.

The combined effects and capabilities of these three major Air Force transformational efforts, plus our ongoing AFCYBER cyber security campaign plan leveraging signals intelligence (SIGINT) and all-source intelligence, industry, National Institute of Standards and Technology, and DISA best practices, provides the Air Force with a full-spectrum, coherent framework for generating threat- and risk-based mission assurance from networks and infrastructure. This mission assurance strategy is girded by an acquisition and life-cycle sustainment enterprise empowered, organized, and resourced to deliver cyber security and resilience for our Air Force.

Cyber Mission Force: Transitioning from Build to Readiness

The Air Force is on track to achieve Full Operational Capability (FOC) for all Service CMF teams by the end of FY 2018. As of 1 May 2017 we have all teams at Initial Operational Capability and over fifty percent at FOC. The FOC criteria are designed to ensure construction of all teams to a common standard and set of work roles. While we remain laser-focused on building and delivering our Service teams to FOC, we have begun, in earnest, to measure and review team readiness across well-established institutional standards such as Personnel, Training, Equipment and Supply. This ongoing road to formal CMF Defense Readiness Reporting System (DRRS) integration will normalize CMF force presentation and force management while generating critical mission capability and capacity gap analysis needed for Commanders to drive force readiness.

At 24th Air Force we know the most critical element in cyberspace operations is not copper or silicon, it's carbon. Our innovative and audacious Airmen are the centerpiece to our AFCYBER capabilities; they have demonstrated time and again their agility and dedication towards generating mission outcomes for our Service, the Joint Force and our Nation. We have thrust them directly from build to battle throughout the CMF build evolutions. Therefore, we remain committed to recruiting, training, developing, and retaining the right cyber talent. We owe it to the incredible men and women that make-up these teams to see they are properly trained, equipped, and prepared for all assigned missions. There must be an evolving dialogue centered on resourcing and procuring the capabilities and capacity required for our CMF to be properly postured for success beyond the build.

"One Force" in AFCYBER

In cyber, we train and fight as one team with all components; Regular Air Force, Air National Guard, and Air Force Reserve. We are delivering cyber forces in support of the Department's CMF framework fully integrated with our Total Force partners in the Air National Guard and Air Force Reserves. These "One-Force" teams are providing United States Cyber Command with capabilities to defend the nation, support Combatant Commanders, and defend the DoDIN. The Air Force's Total Force cyber mission contribution is impressive. They are providing both National and Cyber Protection Teams, Cyberspace Command and Control and a separate Continuity of

Operations Ops Center facility, a Cyberspace workforce training and skills validation course, and niche Industrial Control System cyber-security and defense teams.

The Air National Guard has already completed two extremely successful Cyber Protection Team six month mobilizations in support of United States Northern Command air defense missions and associated key cyber terrain security and defense. These Total Force professionals bring a unique blend of experience and expertise to the full spectrum of cyberspace missions. Many work in prominent civilian positions within the Information Technology industry, which bolsters our mission effectiveness. A prime example from the Washington State Air National Guard is their ability to harness their expertise to establish unique Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) threat prevention and response packages or Unit Type Codes (UTCs) for mobilization and deployment. These ten-person UTCs provide a capability to detect, deter, degrade, and deny an adversary freedom of action within Cyber Physical Systems, Industrial Control Systems, and Critical Infrastructure and Key Resources Networks. Further, the Air National Guard established two units to provide resident initial assessment and cyber skills training as well as delivering on-line cyber training to the Air Force. These vital capabilities allow us to refine training capability requirements that drive future training curriculum design. In addition, the Air Force Reserves, in coordination with our formal cyber school house are focused on development of advanced resident and distributed learning for the CMF.

Operational awareness focused on the mission, Commanders' priorities, and resources are key to forging a lasting partnership with our Total Force brethren. On 26 April, 24th Air Force hosted 27 states Adjutants General, Assistant Adjutants General, and Wing Commanders for the first-ever TAG Cyber Symposium. This historical gathering enabled critical collaboration and information flow regarding personnel, equipment, requirements, and authorities and generated insights into optimizing force presentation and harnessing our citizen Airmen's industry expertise to solve tough cyber operations problems.

Cyberspace operations are a "team sport" and 24th Air Force/AFCYBER is wholly committed to strengthening our relationships with other Air Force partners, our sister Services, interagency counterparts, Combatant Commanders, coalition allies, as well as

civilian industry partners. Given the proximity of our headquarters and close mission alignment, 25th Air Force continues to be a critical strategic partner across all of our missions. The 25th Air Force Commander, Major General B.J. Shwedo, has been a vital force provider and steadfast supporter of the CMF build and operationalization of the cyber domain.

Joint Forces Headquarters-Cyber (JFHQ-C AFCYBER)

Cyberspace is an inherently global domain that impacts every function of our Joint Force. This force is increasingly dependent upon cyber capabilities to conduct modern military operations. JFHQ-C AFCYBER supports assigned Combatant or Joint Force Commanders by providing full-spectrum, all domain integrated cyberspace maneuver and effects in support of their assigned missions. JFHQ-C AFCYBER delivers Cyber IN War, not Cyber War, for our Combatant Commanders. As Commander, I retain Operational Control of assigned Service and joint Cyber Mission Forces providing general support to both United States European Command and United States Strategic Command. We recently concluded a combined Joint, Tier-1 Combatant Command Exercise, Austere Challenge/ Global Lightning 2017, supporting both of these Combatant Commands. United States Cyber Command designated JFHQ-C AFCYBER as the Cyber Component to the Joint Task Force Commander, enabling fully integrated joint planning, maneuver, targeting and fires coordination for cyberspace maneuver and effects operations. Our team effectively integrated within existing, institutional planning, targeting and fires processes to provide cyber effects across the full range of military operations within the exercise. Our capabilities and effects were fully synchronized with the timing and tempo dictated by the supported Commander. Cyberspace domain operations were employed using extant processes, fully integrated with all other classic warfighting domains propagating force awareness, comprehension and intrinsic value across all participants, agnostic of professional pedigree or experience.

Partnerships

24th Air Force also understands the cyberspace domain is primarily provisioned by private industry and our ability to collaborate with our industry partners benefits the

nation's cybersecurity posture. We have developed Cooperative Research and Development Agreements with 25 industry leaders in Information Technology, Defense, and Banking to share and collaborate on innovative technologies and concepts. These collaborative efforts allow us to advance science and technology in support of cyberspace operations, as well as share best practices with industry partners. We continue to leverage this program and are currently in the process of enhancing our partnerships with academia.

In July 2015 the Cyberspace Multi-Domain Innovation Team (CMIT) was established as a partnership between 24th and 25th Air Forces to meet the CSAF's intent to optimize the rapid and cost effective generation of operational all domain integrated effects. CMIT achieves this through the integration and convergence of Cyberspace Operations; Intelligence, Surveillance, and Reconnaissance; and Electronic Warfare capabilities to deliver innovative multi-domain planning support and capabilities. To date, this team has planned and delivered multiple cyber capabilities to ongoing operations and has a number of multi-domain initiatives underway to better enable operations in an Anti-Access/Area Denial (A2/AD) environment.

We are also fortunate to have a long-standing close relationship with San Antonio, Texas, also referred to as "Cyber City USA." The local community has committed significant resources to support the growth of cybersecurity both locally and nationally. Our leadership team participates in a variety of civic leader engagements to share lessons related to cybersecurity. By partnering together, 24th Air Force supports a broad array of programs designed to reach young students, essential to our nation's success in this arena. A good example is the Air Force Association's "CyberPatriot" STEM initiative in which our Airmen mentor cyber teams as part of a nationwide competition involving nearly 10,000 high school and middle school students.

We are also making gains in improving our acquisitions process to support the ever changing technology of cyberspace. The Air Force Life Cycle Management Center has worked diligently to streamline our ability to provide solutions to support our cyber missions through "Rapid Cyber Acquisition (RCA)" and "Real Time Operations and Innovation (RTOI)" initiatives. RCA is part of Air Force Space Command's Integrated Agile Acquisition Construct applied to meeting cyber needs by providing faster solutions

to cyberspace needs through traditional acquisition channels. RTOI are activities that produce critical cyber weapons system and platform modifications, capability improvements, and related changes to operational procedures at the "speed of need."

To enable the execution of these efforts, in April 2016, in partnership with the Air Force Lifecycle Management Center, we established the Cyber Proving Ground (CPG). Its mission is to identify, enable, and accelerate the fielding of innovative, operationally-relevant concepts to improve Air Force, Joint, and Coalition cyberspace operations capabilities. The CPG leverages 24th Air Force's innovation and development capabilities and the existing cyber acquisition capabilities of Air Force Lifecycle Management Center's Crypto and Cyber Systems Division. The CPG is a foundry which brings together cyber operators, air force acquisition and engineering professionals, and private sector vendors with potential solutions to close capability gaps. While CPG projects are small in scope and timeframe, they comprise a broad spectrum of challenges, from complex development and testing efforts, to simple technical evaluations of existing technologies.

I want to highlight two recent efforts from the CPG. First, in just six weeks the CPG developed and fielded the Service's first defensive Solaris capability which enabled our Cyber Protection Teams to secure and defend the Air Force Satellite Control Network. Second, the CPG recently completed development, testing, and fielding of two unique capabilities to support United States Cyber Command's ongoing Joint Task Force Ares operations. Other CPG efforts fielded capabilities that thwarted adversary exploitation of user authentication certificates, the unauthorized release of personally identifiable information, and the blocking of sophisticated intrusion attempts by advance persistent threat actors. These technical solutions were forged, tested and fielded in weeks to months, versus years.

Challenges and Opportunities

As a new and rapidly maturing warfighting domain, cyberspace operations continues to make huge advancements in the operationalization of missions and forces. However, there are significant challenges in our critical path towards delivering required capability and capacity for assigned missions. At the macro-level, these challenges fall into four broad categories; manpower and training, cybersecurity of weapons systems,

key enablers to cyberspace operations, and professionalization of cyberspace domain workforce. These broad categories closely mirror Admiral Rogers' focus areas for United States Cyber Command and the Service Cyber Components. His charges direct us to secure and defend weapons and mission systems and the data that resides on them, as well as increase speed, agility, precision, readiness and lethality of an effectively manned and trained cyber workforce in coordination with Guard and Reserve forces to deliver all domain integrated effects across all phases of operations that support DoD strategy and priorities.

Manpower and Training

Significant manpower shortages across our C2 elements at all echelons hampers our ability to support geographic and functional commands. Manpower deficiencies in our units that operate, secure, and defend our networks force a constant high-pressure, deployed in place operating environment of competing priorities and risk decisions with insufficient force structure to meet critical operational demands. We are actively examining our training pipeline to find smarter more agile methods which get our operators to their units and on mission faster. In 2015 we added a local San Antonio detachment to our cyber school house to increase training capacity. The detachment is crucial in enhancing formal training throughput and efficacy due to the proximity to the majority of Air Force CMF units and their cyber weapon systems. Since June 2015, the detachment has graduated 518 CMF operators and saved one million dollars per year in TDY costs by collocating the training with the operational units. Formal cyberspace operations training must remain rigorous and comprehensive enough to meet operational requirements but also agile and responsive enough to accommodate the pace of change in the cyber domain.

The Service Staff in conjunction with Air Education and Training Command are currently developing custom Air Force Specialty Code training tracks based on a modular syllabus that utilizes the latest training assessment innovations and provides placement flexibility through the training pipeline. The concept allows Airmen to "test-out" of portions or modules of the curriculum. This methodology provides incentives and opportunities to our Airmen who possess an advanced cyber aptitude, whether via formal or informal training or education, to advance through the pipeline and arrive on

station at an operational unit in a significantly shorter time frame. In order for this concept to be effective, resourcing is required to design and validate assessment tools and develop an agile and responsive curriculum development framework that keeps pace with the advancement of technology, tradecraft, and our adversaries.

Cybersecurity of Weapons Systems

There are insufficient weapons system sustainment dollars going towards system cyber security and defense. The majority of all sustainment dollars today goes toward functional capability upgrades in any mission or weapons system program. Our current process of "bolting on" weapons system cyber security after the fact, levies excessive mission-risk and is extremely manpower and resource intensive to properly secure and defend the system. It is more complex and expensive to defend mission systems where there is no inherent or "baked in" cybersecurity framework. As previously mentioned, the CROWS office is getting after this today as directed by the NDAA, but much more needs to be done from a resource and execution perspective.

Key Enablers

The Department has begun planning for and resourcing a multiple phenomenology approach to access. Each Service is exploring multiple pathways to get to the target and deliver effects against our adversaries in cyberspace. The Air Force is also planning and provisioning for its own organic platform and tool development capabilities, separate and distinct from NSA. This will ensure assigned cyberspace mission priorities and requirements are being met. Critical to accessing the target with the appropriate tools to deliver the desired effect is timely, relevant, domain specific, all-source intelligence.

While achieving and maintaining a depth of knowledge in cyberspace is technically challenging, all source Target System Analysis (TSA)s that are domain agnostic is a proven approach to providing timely, relevant intelligence support to operations. The Intelligence Community (IC) must perform this function due to the vast amount of resources and the ability to leverage existing partnerships outside the Department and the United States Government. The methodology employed purposely resembles target development in any other warfighting domain. A thorough understanding of the Commander's intent, specifically the objectives and effect desired

for a particular target set is required. Center of Gravity analysis is conducted to analyze the functions and interconnectivity of those components critical to the target. Systems engineering and network analysis is developed to map out the key terrain within the target, to enable operators to conduct Intelligence Preparation of Environment (IPOE) and refined Target Development. Based on the analysis and reporting from the IPOE, the operators develop a strike package based on an understanding of the target environment and the tools and capabilities they have developed in order to deliver the desired effects. The current approach of contracting these cyber TSAs has been successful, but we view it as a temporary solution until the IC transforms their on-going intelligence support to cyber analysis and resourcing challenges and takes on this critical intelligence requirement in earnest.

Professionalization of the workforce

The Air Force established a Cyber Project Task Force to monitor progress, identify challenges, and collaborate on manpower and personnel efforts to "get after" building the Air Force portion of the CMF. The Air Force also instituted a Service-wide policy to encourage back-to-back CMF tours for our CMF-trained personnel, thereby ensuring proper return on investment. Furthermore, the Air Force recognized the positive value of embedding limited CMF-trained personnel back into Service non-CMF cyber positions, in order to better operationalize the total Service cyber enterprise. Although, these cross-pollinated CMF-trained personnel may not have specific CMF-related or associated jobs, they are assigned to cyberspace-related positions growing their depth and breadth of operational expertise. Finally, the Air Force also has the responsibility to develop our portion of the CMF to meet Operational Commanders' requirements in a method that also ensures Air Force Cyber Airmen stay competitive with long-term career projections and a "Path to Greatness" for cyberspace Airmen. In addition, cyber Airmen may attend professional developmental opportunities such as Air Force Institute of Technology, Computer Network Operations Development Program, or the Air Force Weapons School, all of which will positively impact the operationalization of the cyberspace domain within the Air Force and in turn, the future of the CMF.

Conclusion

I am proud of the tremendous strides made to operationalize cyber capabilities in support of joint warfighters and defense of the nation. Despite the challenges of growing and operating across a contested and diverse mission set with a rapidly maturing work force, it is clear Air Force networks are better defended, Combatant Commanders are receiving more of the critical cyber effects they require, and our departments' critical infrastructure is more secure due to our cyber warriors' tireless efforts. They truly are professionals in every sense of the word.

Congressional support was essential to the substantial operational progress made and will only increase in importance as we move forward. Without question, resource stability in the years ahead will best enable our continued success in developing Airmen and maturing our capabilities to operate in, through and from the cyberspace domain. Resource stability will also foster the innovation and creativity required to face the emerging threats ahead while maintaining a capable cyber force ready to act if our nation calls upon it.

I am honored and humbled to command this magnanimous organization and look forward to a thorough and continuing dialogue.