DEPARTMENT OF THE AIR FORCE

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

March 13, 2018

NOT FOR PUBLICATION UNTIL RELEASED BY
SENATE ARMED SERVICES COMMITTEE
SUBCOMMITTEE ON CYBERSECURITY
U.S. HOUSE OF REPRESENTATIVES

Introduction

Chairman Rounds, Ranking Member Nelson, and distinguished members of the Subcommittee, thank you for the opportunity to appear before you today, along with my fellow Service Cyber Component Commanders. I look forward to discussing the Air Force's significant progress in advancing full-spectrum cyberspace operations and our contributions to joint operations globally. I have the distinct honor to lead the audacious men and women of the 24th Air Force, Air Forces Cyber (AFCYBER), and Joint Forces Headquarters Cyber (JFHQC) Air Force. Our headquarters is located at Joint Base San Antonio-Lackland, Texas and we have over fifteen thousand Total Force Airmen and civilians on-mission around the world, diligently increasing our capability to deliver full spectrum cyber capabilities and effects in support of the Air Force, the Joint Force, and our Nation.

AFCYBER warriors are operating globally as a maneuver and effects force in a contested domain, delivering cyber superiority for our Service and in support of our joint partners. Our forces exist to preserve our freedom of maneuver in, from, and through 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 tactics, techniques, and procedures (TTPs) 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 Cyber Command. These ready forces plan and execute all-domain integrated, full-spectrum, cyberspace operations in support of assigned Service and Combatant Command missions. Finally, under my third hat, as Commander, JFHQC Air Force, 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. At 24th AF/AFCYBER, we execute our 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. In 2012, 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. Our reliance on cyberspace continues to grow and we are still scaling capacity to execute this expansive mission requirement. We are

working closely with Headquarters Air Force and Army Research Laboratories to ensure our threat- and risk-driven defensive operations preserve our freedom of maneuver in, from, and through cyberspace while denying our adversaries the same. In 2016, we instituted the Air Force Information Network Defense Campaign Plan and have since made great strides in improving our cybersecurity posture and compliance with both USCYBERCOM orders and industry-recognized cyber hygiene best practices.

A major cyberspace security and defense success over the last year has been the employment of the Automated Remediation and Asset Discovery (ARAD) capability suite across the AF enterprise. 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 across our AF network in a matter of seconds to minutes vice days to weeks using previous capabilities. In May 2017, at first onset of the WannaCry Ransomware attack, our cyber crews employed ARAD capabilities to quickly identify, prioritize and secure all vulnerable systems across our enterprise terrain within hours; resulting in zero infections on Air Force networks. By contrast, the 2013 Heartbleed virus remediation effort took 8 months to achieve the same results. The demonstrated operational power and potential of ARAD is truly revolutionary, and we are diligently experimenting, evolving, and developing operational employment concepts, use cases, and applications to close key mission-capability gaps in close partnership with the Tanium experts.

Cybersecurity in the 21st Century

In the contested cyberspace domain, threats are growing rapidly and evolving. Our adversaries are acting with precision and boldness; utilizing cyberspace to attack the United States below the threshold of armed conflict; imposing great costs on our economy, national unity, and military advantage. In this ever-shifting and competitive terrain, we must remain vigilant with cyber hygiene, cyber security, and threat-specific defensive operations in order to compete, deter, and win.

The Air Force has invested in the creation, fielding and sustainment of seven cyber weapon systems designed to provide a tiered global defense of the Air Force Information Network. We have also fielded defensive cyber maneuver forces and capabilities to engage threats able to bypass defenses, and offensive cyber forces and capabilities to provide all-domain integrated operational effects to Combatant Commanders.

Last year, I discussed three transformational efforts that 24th Air Force, in collaboration with our Service staff and Major Commands, developed and implemented in order to 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 Enterprise Information Technology as a Service (EITaaS), 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. 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.

Over the past year the EITaaS concept has evolved. EITaaS 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 basic services to commercial and industry partners. The Chief of Staff of the Air Force has approved this plan of action and requested an accelerated implementation starting in FY18. The Air Force has identified the first seven bases to implement EITaaS to determine the service planning necessary to capture further requirements, learn appropriate command and control and security provisions and transition Airmen from NetOps missions and functions to cyber-based system defense and mission assurance. A companion effort within EITaaS is our on-going Cloud Hosted Enterprise Services (CHES).

Cloud Hosted Enterprise Services (CHES), started in 2016, provides collaboration (e-mail, Skype for business, SharePoint) as Software-as-a-Service. It is currently securely hosting over 187,000 user accounts across ten bases. This service delivery model has been praised for improved network performance, reliability and scalability. EITaaS will integrate into on-going Joint Information Environment (JIE).

Joint Regional Security Stack (JRSS) migrations and fielding continues in close partnership with the United States Army and the Defense Information Services Agency (DISA). All DoD components will ultimately utilize JRRS. To date, we have successfully migrated four

regions, to include roughly four hundred thousand users across 105 locations. While JRSS still requires TTP development and a more mature operational employment framework, this joint, shared security standard provides state of the art cyber security capabilities at our Service (Tier-2) AFNET gateway boundaries, continuing to add strength to our layered defense.

The CMF Cyber Protection Teams (CPTs) and Air Force Mission Defense Teams (MDTs) continue to provide active cyber defense at all echelons of Air Force organizations; delivering enterprise mission assurance in a contested domain even in the presence of a maneuvering enemy. Mission Defense Teams (an on-going "pilot" program across all Major Commands) are small 4-6 person teams; trained, equipped and task-organized to survey, secure, and protect key cyber terrain at wing and below in order to deliver cyber-based mission assurance for unit's assigned missions and weapon systems. This initiative employs a Commander and mission-driven force employment model. Mission Defense Teams employ 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. Since 2016, the Air Force has executed 45 Mission Defense Team "Pathfinder" initiatives across a diverse set of Air Force missions and organizations to test and validate the operational concept and cyber defensive tool-set requirements. These "Pathfinder" units focused on functional mission analysis to identify key-cyber terrain, mission-planning, and network characterization. Leveraging the "Pathfinder" lessons learned, the Air Force is now working to optimize the MDT force construct, training needs, intelligence support requirements, and tool-set. MDT efforts will continue to be synchronized with our CSSP, CPT, and CROWS missions to provide an integrated, layered security and defensive posture for Air Force weapon systems.

The third transformational effort is Air Force Materiel Command's Cyber Resiliency of Weapons Systems, or CROWS office (in response to the 2016 NDAA section 1647 requirement). Their on-going 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 has 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. Based on the NDAA language, the Joint Staff required the Air Force to evaluate 50 legacy weapon systems. To date, the Air Force has begun 23 weapon system evaluations and is on track to complete all 50 by the end of 2019 (deadline set by NDAA.) 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. While still relatively new, the CROWS Cyber Incident Coordination cell has proved invaluable throughout this past year, working in coordination with 24th Air Force, as vulnerabilities have been found in cyber key terrain of mission systems. The office will continue to mature and enhance the cyber security posture of new and existing weapon systems.

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 for our networks, infrastructure and mission/weapon systems. This mission assurance strategy is reinforced by an acquisition and life-cycle sustainment enterprise empowered, innovating, and resourced to deliver cyber security and resilience for our Air Force.

AF Data Office

Data is the digital currency that underpins multi-domain operations, decision-making and command and control. For a Service to be a leader in the application of artificial intelligence to increase warfighting resilience and lethality, it must first be a leader in data. To this end, the Air Force has stood up the Air Force Data Office, and appointed a Chief Data Officer, Maj Gen Kim Crider USAFR. The Air Force is the first Service to create an enterprise level Data Office reporting directly to the Service Secretary.

The Air Force Data Office has developed a "VAULT" strategy, centered on ensuring relevant data is—Visible, Accessible, Understandable, Linked, and Trustworthy. They are diligently working on data science application use-cases across a cross-section of Air Force missions and functions to generate both visible quick-wins and a greater understanding of the required enterprise-data architecture and operational employment concepts required to deliver desired outcomes. Data driven multi-domain Command and Control is the path to integrated Joint operations whose operational timing/tempo lives inside our adversaries "OODA" loop,

overwhelming their decision cycles, delivering the operational advantage and initiative to our Joint Forces.

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 March 2018, 35 of 39 Cyber Mission Force (CMF) teams have declared FOC, and the four remaining teams are expected to declare FOC by June 2018, 3 months ahead of the deadline. AFCYBER has developed a team-by-team, name-by-name plan that ensures all teams will achieve FOC on time. This significant milestone is due to the years of hard work by the Service and USCYBERCOM, with the support of Congress.

While we remain laser-focused on building and delivering our Service teams to FOC, we continue, in earnest, to generate and review team readiness leveraging well-established institutional standards and metrics (Personnel, Training, Equipment and Supply.) We are working with our Service and USCYBERCOM to institutionalize formal CMF Defense Readiness Reporting System (DRRS) definitions, metrics and integration. This will normalize CMF force presentation and force management while generating critical mission capability and capacity gap analysis needed for Commanders to drive force readiness. As Admiral Roger's stated, "Commissioning a warship – while an important event – does not make that ship mission ready." Readiness and lethality are paramount. The Air Force continues to work to recruit and retain top talent, develop modularized and agile training, build our own military operations infrastructure, as well as deliver organic combat capabilities to the Joint war fight (these initiatives are discussed below). We have made great strides, but a lot of work still needs to be

done to ensure our CMF crew members are proficient at their duties and the whole team is ready and able to perform assigned missions and tasks.

The Air Force has taken a conscientious and deliberate approach to building our Service cyber workforce. While CMF remains the #1 priority, the Air Force is actively developing cyber Airmen and civilians that have the proper balance of technical and tactical/operational competence needed to fully integrate cyberspace into joint military operations. The Air Force is still building the cyber bench, employing a deliberate approach to human-capital professional force development.

At 24th Air Force we know the most critical element in cyberspace operations is not copper or silicon, its carbon. Our innovative and audacious Airmen are the centerpiece to our AFCYBER capabilities, our most powerful weapon system by far; 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. I must thank Congress for increasing our agility in shaping our workforce; the new Cyber Excepted Service authorities will help us recruit, manage, and retain cyber expertise in a highly competitive talent market. With support from the NDAA, the Air Force now has the ability to directly commission cyberspace operations officers, the first two of whom will be entering the force early this year, one as a Second Lieutenant, and one as a First Lieutenant. We have also instituted retention bonuses for officers and enlisted within the cyber career field in order to preserve the experience of our trained and ready airmen. 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

Air Force Cyber trains and fights as one Total Force team with all components; Regular Air Force, Air National Guard, and Air Force Reserve. Across 24th Air Force, we employ more than eleven thousand full-time and part time reservists, providing support for training, intelligence, operations, and command and control, incorporating units in 31 states.

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. For CMF, the Air Force has 15 Air National Guard squadrons supporting two Cyber Protection Teams and one National Mission Team. At the conclusion of our CMF build-phase, the Air Force's Cyber Protection Force will have a 50% surge capacity built-in with 10 Cyber Protection Teams in ready-reserve status and available during times of crisis. By the end of Calendar Year 2018, all 15 Air National Guard squadrons will have been mobilized and have "on-mission" experience under their belts. Similarly, the Air Force Reserves provide the equivalent of a full Cyber Protection Team and are currently integrated with Active Duty forces. This represents a

significant portion of the Air Force's overall contributions and will draw on more than 1,100 Reserve Component members. These Total Force professionals bring a powerful pedigree of experience and expertise across the spectrum of cyberspace missions. Many have years if not decades of experience working in prominent civilian IT, Infrastructure and Industry positions, which bolsters our cyber mission-effectiveness on many levels.

The Air National Guard has already completed five extremely successful Cyber Protection Team six-month mobilizations (254 cyber operators) in support of United States Northern Command's air defense missions and associated key-cyber terrain security and defense.

The Reserve's 854th Cyber Operations Squadron in conjunction with the Tennessee Air National Guard provide over 300 personnel to augment and provide continuity of operations for the Air Force's Cyber Operations Center.

The Total Force also plays a crucial role in our Engineering and Installation (E&I) and Combat Communications capabilities; consisting of over 75% of the Air Force's available E&I and Combat Communications personnel. 24th Air Force E&I Citizen Airmen have been on site executing USSTRATCOM's new HQ cabling and IT-network/systems fit-out for over 3 years, delivering an estimated DoD cost avoidance of over $400M over original contract bids. Our 5th Combat Communications Group continues to deliver and extend combat capabilities at the tactical edge. In 2017, our 5th Combat Communications Group deployed more than 131 personnel to over 25 sites in 14 countries. In February 2017, the 5th Combat Communications Group deployed Airmen to stand up the initial communications at a bare base in Syria. The team provided communications support to the site's Senior Airfield Authority who managed the ramp

and airspace for the only U.S. military logistics hub in country and home to units from the Army, Marine Corps, Special Operations, and Department of State. In FY17, the Air Force garnered $42.7M to modernize the capabilities for 23 combat communications units. These new capabilities empower our combat communications forces to be better prepared and more efficiently support Combatant Commanders' worldwide.

In June 2018, 24th Air Force will host the second-annual state Adjutants General, Assistant Adjutants General, and Wing Commanders Cyber Symposium. Improving operational awareness focused on the mission, Commanders' priorities, and resources are key to forging a lasting partnership with our Total Force brethren. This gathering will continue to enable critical collaboration and information flow regarding personnel, equipment, requirements, and authorities and generate 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 Mary O'Brien, has been a vital CMF force provider and steadfast "Wingman" as we partner to generate enduring force readiness and operationalization of the cyber domain.

Support to Combatant Commands

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 AF supports assigned Combatant and subordinate Joint Force Commanders by providing full-spectrum, all domain integrated cyberspace maneuver and effects in support of their assigned missions. JFHQ-C AF delivers "Cyber IN 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 continue to operationalize and mature cyber operations into Tier-1 Combatant Command Exercises, concluding our third exercise in January. Our continued involvement in major exercises enables fully integrated joint planning, maneuver, targeting and fires coordination for cyberspace maneuver and effects operations. It also drives Combatant Command awareness and trust of cyberspace capabilities. 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.

The Chairman of the Joint Chiefs of Staff furthered this goal by updating the cyberspace operations command and control framework last fall, directing USCYBERCOM establish Cyber Operations – Integrated Planning Elements (CO-IPEs) at each Combatant Command. JFHQC AF has administrative control of the CO-IPEs at USEUCOM, USSTRATCOM, and USTRANSCOM to plan, synchronize, integrate, and de-conflict cyber operations with Combatant Command plans and operations. We are partnering closely with our Service to build and operationalize these new units to full operational capability within the next three to five years.

Partnerships

24th Air Force 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 20 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.

We employ private sector technology and expertise to build, operate, secure, and defend the Air Force Network. Right now, within my headquarters and operations center, we have

experts from leading technology companies (Microsoft, Cisco, Symantec, AT&T) working hand in hand to develop solutions to both current problems and future concepts.

In cyberspace, innovation is crucial. Over the past two years, we have synchronized with cyber innovation centers of excellence across the Service, Department, and Nation, including the Air Force Academy CyberWorx, Defense Digital Service (DDS), Defense Innovation Unit Experimental (DIUx), the Cyber Proving Ground, Air Force and National Research Labs, the Federal Bureau of Investigation (FBI), and Defense Advanced Research Projects Agency (DARPA.)

In December 2017, in cooperation with Air Force Defense Digital Service, we launched the second instantiation of our Hack the Air Force program. A bug bounty program, Hack the Air Force continues to showcase how a diverse, crowdsourced pool of private sector, ethical hackers can help quickly identify critical security vulnerabilities across public facing Air Force assets. This event included 24 top hackers working alongside 24th Air Force cyber operators to both hack and remediate vulnerabilities in real-time. Hackers hailed from 32 international partner nations, including members of the North Atlantic Treaty Organization, Five Eyes nations, and Sweden. This event was a major success; discovering over 106 valid vulnerabilities and allowing our cyber operators to gain from the expertise of the hackers as well as garner real time remediation experience.

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 "Cyber Patriot" 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.

Challenges and Opportunities

As a new and rapidly maturing warfighting domain, cyberspace operations continue to make huge advancements in the operationalization of missions and forces. However, there are many 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; (1) manpower and training, (2) cybersecurity of weapons systems, (3) key enablers to cyberspace operations, and (4) professionalization of the 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. While the primary challenges remain the same, and acknowledging there is much more to do, the Air Force has made and continues to make great progress along these lines of effort.

Manpower and Training

Success in our missions depends on a trained and ready force. As stated above, congressional support has been instrumental in increasing our agility in scaling and shaping our workforce. A dedicated Civilian Cyber Recruiting cell was established at the Air Force Personnel Center in January 2017 to focus on cyber recruiting. In 2017, the cell completed 30 recruiting events including cyber collegiate competitions and technology events. The Air Force has expedited civilian cyber hiring through the use of Direct Hire and Expedited Hire appointments, reducing the hiring time by about 35%. For our military members, we are creating aptitude assessments to find the right personnel and modifying our cyber personnel paths including monetary incentives to retain them. Monetary incentives range from $300 per month for our new enlisted cyber operators to $60,000 over the period of four years for some of our officers.

We continue to make great strides, but challenges still remain. As discussed last year, manpower deficiencies in our units that operate, secure, and defend our networks still 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. The EITaaS effort will help alleviate some of this burden, but should not be viewed as a complete panacea.

In FY19, USCYBERCOM transitions the CMF training mission to the Services. In preparation for the receipt of this mission, we continue to make our training pipeline more

adaptive and responsive to operational needs. We have enhanced our training capacity, increasing the annual training throughput of our enlisted cyber initial skills training schoolhouse by 54% (211 to 324 students per year) beginning in CY17. The Air Force also stood up a local San Antonio detachment to our advanced cyber formal training unit effectively doubling capacity there. This effort has allowed the Air Force to execute the CMF TFI Strategy and keep pace with the ever-increasing cyberspace operator requirements outside of CMF. Additionally, the Air Force is developing specialized courses to deliver the right training at the right time to our cyber operators. We have created a new Cyber Intelligence Initial Qualification Training and a provisional offensive cyber operations formal training unit. In June 2018, 24th Air Force will host our first interactive operator course utilizing our organic military cyber operations platform. Looking toward the future, we are building a $14.2M, 36,000 square foot schoolhouse facility at our main cyber formal training unit at Hurlburt Field, Florida. Groundbreaking was on 10 August 2017 for a scheduled completion in late FY19.

The Service Staff in conjunction with Air Education and Training Command are currently developing custom Air Force Specialty Code (AFSC) 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 with intrinsic cyber competency 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 ready to contribute to our mission. In order for this concept to be effective, resourcing is required to design and validate

aptitude 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 Weapon Systems

We must continue to increase investment 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 adversely impacts all three critical systems-acquisition and sustainment attributes: cost, schedule, and performance. 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 to generate the tempo and scale of action necessary to secure our expansive weapon system portfolio.

Key Cyber Enablers

The Department has begun planning for and resourcing a multiple phenomenology approach to generating "access" to required cyber-space. Each Service is exploring multiple pathways to get to the target and deliver effects against our adversaries in cyberspace. The Air Force has planned and is provisioning its own organic military cyber operations platform, for Joint CMF use, separate and distinct from NSA. The Air Force's organic cyber military operations platform completed its proof of concept mission in September 2017 and is now being

utilized by our CMF forces. Its continued development, along with agile and responsive tool development capabilities, will ensure assigned AF and Joint CMF mission priorities and requirements are being met.

Professional Development of our Workforce

The Air Force established a Cyber Project Task Force (PROTAF) 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 enforce back-to-back CMF tours for our CMF-trained personnel, thereby ensuring proper return on investment, and is reviewing the current Active Duty Service Commitment model for certain cyber operations work roles to ensure proper return on investment. Furthermore, the Air Force recognized the positive value of spreading cyber-mindedness and experience across our AF enterprise, just like air and space operations, to ensure cyber competency across all mission areas and corporate activities.

Risk

In order to become the challenger in the cyber domain and operate effectively across the range of military operations, we must address our current risk posture. The natural evolution and progression of cyberspace operations (maneuver and effects forces) from NSA's long-standing SIGINT and CNE missions (intelligence forces) and operations brings with it a well-established

intrinsic risk posture to gird foreign intelligence collection operations in an extremely congested and contested operational Domain.

In this light, today's cyberspace operations are overly risk-driven vice being mission-driven and risk-informed more in line with the other classic domains of warfare. USCYBERCOM and the Service Cyber Components require a more responsive and agile mission-oriented risk framework which delivers the speed, agility and operational fighting tempo needed to seize the initiative and advantage in our battle space.

We must challenge the Domain's outmoded concepts of sovereignty, attribution, and intelligence gain/loss calculus which overly constrain our ability to achieve cyberspace superiority across assigned missions and functions. Our risk framework needs to drive operational outcomes and be properly informed by both the war-winning and risk mitigation imperatives. We are in constant contact in cyberspace with multiple adversaries daily. We must persist, at times we must fallback and cede terrain, and we must accept some level of calculated capability attrition (access, platform, tools), all while harnessing our innate National capability and capacity to out think, out maneuver and out punch our adversaries. This is the recipe for eroding their confidence in cyberspace, imposing costs, and challenging their belief system for achieving benefit thru malicious cyber actions. In parallel, we need to effectively and transparently communicate the legitimacy of our actions in/from/thru cyberspace so our Nation and our Allies fully understand and support the actions we take to secure and defend our combined National Security interests, our freedoms and our unmatched quality of life.

Conclusion

I am proud of the tremendous strides we are making 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 capabilities and effects they require, and our departments' critical infrastructure is more secure due to our cyber warriors' tireless efforts. They are true 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 while growing our capability and capacity 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.