AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 115–674, PT. 8

DEPARTMENT OF DEFENSE AUTHORIZATION FOR APPROPRIATIONS FOR FISCAL YEAR 2019 AND THE FUTURE YEARS DEFENSE PROGRAM

HEARING

BEFORE THE

COMMITTEE ON ARMED SERVICES
UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

ON

S. 2987

TO AUTHORIZE APPROPRIATIONS FOR FISCAL YEAR 2019 FOR MILITARY ACTIVITIES OF THE DEPARTMENT OF DEFENSE AND FOR MILITARY CONSTRUCTION, TO PRESCRIBE MILITARY PERSONNEL STRENGTHS FOR SUCH FISCAL YEAR, AND FOR OTHER PURPOSES

PART 8
CYBERSECURITY

MARCH 13, 2018

Printed for the use of the Committee on Armed Services

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
41–250 PDF WASHINGTON : 2020

COMMITTEE ON ARMED SERVICES

JOHN MCCAIN, Arizona, *Chairman*

JAMES M. INHOFE, Oklahoma	JACK REED, Rhode Island
ROGER F. WICKER, Mississippi	BILL NELSON, Florida
DEB FISCHER, Nebraska	CLAIRE MCCASKILL, Missouri
TOM COTTON, Arkansas	JEANNE SHAHEEN, New Hampshire
MIKE ROUNDS, South Dakota	KIRSTEN E. GILLIBRAND, New York
JONI ERNST, Iowa	RICHARD BLUMENTHAL, Connecticut
THOM TILLIS, North Carolina	JOE DONNELLY, Indiana
DAN SULLIVAN, Alaska	MAZIE K. HIRONO, Hawaii
DAVID PERDUE, Georgia	TIM KAINE, Virginia
TED CRUZ, Texas	ANGUS S. KING, JR., Maine
LINDSEY GRAHAM, South Carolina	MARTIN HEINRICH, New Mexico
BEN SASSE, Nebraska	ELIZABETH WARREN, Massachusetts
TIM SCOTT, South Carolina	GARY C. PETERS, Michigan

CHRISTIAN D. BROSE, *Staff Director*
ELIZABETH L. KING, *Minority Staff Director*

SUBCOMMITTEE ON CYBERSECURITY

MIKE ROUNDS, South Dakota, *Chairman*

DEB FISCHER, Nebraska	BILL NELSON, Florida
DAVID PERDUE, Georgia	CLAIRE MCCASKILL, Missouri
LINDSEY GRAHAM, South Carolina	KIRSTEN E. GILLIBRAND, New York
BEN SASSE, Nebraska	RICHARD BLUMENTHAL, Connecticut

CONTENTS

MARCH 13, 2018

DEPARTMENT OF DEFENSE AUTHORIZATION FOR APPROPRIATIONS FOR FISCAL YEAR 2019 AND THE FUTURE YEARS DEFENSE PROGRAM

TUESDAY, MARCH 13, 2018

U.S. SENATE,
SUBCOMMITTEE ON CYBERSECURITY,
COMMITTEE ON ARMED SERVICES,
Washington, DC.

CYBER POSTURE

The subcommittee met, pursuant to notice, at 2:31 p.m. in Room SR–222, Russell Senate Office Building, Senator Mike Rounds (presiding) chairman of the subcommittee.

Members present: Senators Rounds, Sasse, Nelson, McCaskill, Gillibrand, and Reed.

OPENING STATEMENT OF SENATOR MIKE ROUNDS

Senator ROUNDS. The Cybersecurity Subcommittee meets today to receive testimony on the Cyber Posture of each branch of our Armed Forces, from Vice Admiral Michael Gilday, Commander, Fleet Cyber Command; Lieutenant General Paul Nakasone, Commander, Army Cyber Command, and nominee to be the next Commander of the United States Cyber Command, and Director of the National Security Agency; Major General Loretta Reynolds, Commander, Marine Forces Cyber Command; and Major General Christopher Weggeman, Commander, Air Force Cyber.

At the conclusion of Ranking Member Nelson's remarks, we will ask our witnesses to make their opening statements. After that, we'll give each of our members 5 minutes to ask questions of our witnesses.

As we approach full operational capability later this year, maturation of the Cyber Mission Force continues at an impressive pace. According to Admiral Rogers' testimony a couple of weeks ago, we are on pace to reach that milestone earlier than planned. This, along with the many other advances we see as the Department takes what was once a niche capability and transforms it into a multifaceted warfighting discipline, is the result of your hard work. We thank you for your leadership.

Despite the successes, however, challenges remain as your focus now shifts from building a first-of-its-kind force to sustaining one. In particular, that sustainment will require a robust pipeline of talent ready to take the reins as soldiers and civilians move to other

disciplines, are promoted, or separate from the military to take cyber jobs in the private sector.

Last year, we heard about the 127 Air Force cyber officers who, after completing their tour on the Cyber Mission Force, departed the Cyber Mission Force. We understand that was an isolated incident and that each of the Services has enhanced its focus on how it manages it force. Just recently, the Marine Corps announced that it was creating a cyberspace occupational field to address some of these challenges. I think we all expect this to be a perpetual challenge, and we look forward to hearing how you are working together, sharing ideas, and pursuing creative approaches to make certain that we develop the bench strength that we require.

When it comes to providing the cyberweapons that the force will need to deter and defend its cyberspace, there, too, is significant room for improvement. As we heard from Admiral Rogers a couple of weeks ago, we are not where we need to be. Numerous niche capabilities exist today; however, across the enterprise, the capabilities for training and conducting operations are in the earlier stages of development and won't be delivered for some time. The force will undoubtedly be hollow in the near term, and it is incumbent upon each of you to deliver those fundamental tools and capabilities as quickly as possible to make certain that the impressive gains you have made in training the force are not lost because of this lack of cyberweapons. We have been largely critical of the Department regarding this failure in the past, but we do see progress.

The fiscal year 2019 budget requests included $1.8 billion for the manning, training, and equipping of the Cyber Mission Force. The Army and the Air Force requested approximately $700 million each in fiscal year 2019. The Navy request, however, was only $318 million and is less than half the request of its peers. Both the Army and the Air Force have committed to developing foundational capabilities, like the Army's persistent cyber training environment and the Air Force's unified platform. We look forward to hearing more from the Navy and the Marine Corps as to why, legitimately, their funding requirements are substantially less than the other Services.

I think our hearing would be incomplete without some discussion of the Services' offensive and defensive cyber capabilities. Of particular interest to me is the Services' offensive capabilities in the context of the report of the Defense Science Board Task Force on Cyber Deterrence, which was published in February 2017, just over a year ago. As we know, that report notes the importance of a strong cyber deterrent for the next 10 years, a period during which we will not have the defensive capability to defeat our peer adversaries' offensive capabilities. I would be interested in how the Services are focusing to meet that challenge and policy issues—policy issues—that may be inhibiting their ability to do so.

Finally, I would like to know how the Services assess their capabilities to provide support to civil authorities.

Let me close by expressing our gratitude to the witnesses. Yes, issues do remain, but the progress made in the past 8 years is a testament to the advocacy and leadership of each of you and your predecessors. Thank you again for your service and your willingness to appear today before our subcommittee.

Senator Nelson.

STATEMENT OF SENATOR BILL NELSON

Senator NELSON. Thank you, Mr. Chairman.

I want to hit three issues for you all to contemplate and to respond to.

The first is just how disorganized the Department of Defense is when it comes to information warfare or information operations. Officially, doctrine recognizes that information operations include cyber, psychological, electronic, and public affairs. There's even an organization called Joint Information Warfare Center, and at the level of the Military Services represented here today, there is some integration of all of these elements. But, above that level, these elements are all dispersed. Cyber Command doesn't have the responsibility for information operations, which, these days, are conducted largely through cyberspace, and information operations and electronic warfare are the responsibility of still other parts of the Department. Now, why does this matter? Because Russia's information operations troops conduct both technical and cognitive operations in an integrated way. We conduct information operations in support of commanders at the tactical level. Putin and other adversaries are coming at us at the strategic level in so-called peacetime. I'm afraid that we are ceding the playing field. I look forward to you all giving us your answers to this.

The second issue is the slow pace of progress in equipping the cyber units that we have built. We've manned and trained our cyber units, but we still lack basic joint capabilities for command and control, the clandestine network infrastructure needed to maneuver our forces in cyberspace, and the tools and weapons that they need.

The third issue is: we have to squarely face the reluctance to use military cyber units to respond to attacks against us, to confront Russian hackers and trolls, to harass North Korean operators who attack Sony, and to disrupt ISIS [Islamic State of Iraq and Syria] Internet operations outside areas of declared hostilities. We're not conducting our own information operations to defend against and to deter acts—attacks and acts on us and our allies.

This is not just about Russia. It's about differing views among all the parts of our Government about what constitutes traditional military activities. We have to change this. Our forces can't just watch our adversaries in cyberspace. I applaud General Weggeman for stating, in his prepared comments, and I quote, "We must challenge outmoded concepts of sovereignty, attribution, and intelligence gain/loss calculations which overly constrain our ability to achieve cyberspace superiority," end of quote.

We're all concerned about these threats, but that concern has not yet been matched by action. I want to hear what each of you think, and I realize, as stated to us by the four-star Commander of Cyber Command, he hasn't been given the direction. So, I understand the constraints that you have. But, we've got to get this out on the table. I hope we can start today.

Thank you, Mr. Chairman.

Senator ROUNDS. Thank you, Senator Nelson. I think you do a good lead-in to a lot of not just the capabilities that we've got, but to the policy issues we have to address, as well.

I'm not sure how you would like to proceed, or in what order you would like to proceed. If there is a preference, I would allow our witnesses to make that determination.

Lieutenant General Nakasone, have you—would you care to begin, sir?

STATEMENT OF LIEUTENANT GENERAL PAUL M. NAKASONE, USA, COMMANDING GENERAL, UNITED STATES ARMY CYBER COMMAND

Lieutenant General NAKASONE. Thank you, Senator.

Senator Rounds—Chairman Rounds, Ranking Member Nelson, and members of the subcommittee, it's honor—it's an honor to be here, alongside my joint teammates, representing U.S. Army Cyber Command.

My testimony today focuses on the progress Army Cyber Command has made since May 2017, when I last sat before this subcommittee.

Today, the Army's 41 Active Cyber Mission Force Teams are fully operational, on mission, equipped, and delivering capabilities to joint and Army commanders in contingency operations across the globe. With the initial build of the Army Cyber Mission Force complete, our cyber is now focused on sustaining and measure readiness and building the Army's 21 Reserve component teams. All 21 Reserve component teams, which are now part of the Cyber Mission Force, will reach initial operational capability by 30 September 2022, and full operational capability by 30 September 2024.

We continue to make our networks more secure and more dependable through convergence, modernization, and standardization. A key priority is updating Army computers to a more secure operating system, a system known as Windows 10. Over the past 12 months, the Army has already upgraded over 95 percent of its approximately one million computers.

Regarding training, the Army Cyber Center of Excellence is now teaching all cohorts from all components and preparing to integrate the electronic warfare force into the cyber career field. The Army also continues to guide program management for the joint persistent cyber training environment. We are leveraging existing infrastructure and resources to integrate the best government off-the-shelf and commercial off-the-shelf solutions. Construction on the Army Cyber Command Headquarters Complex at Fort Gordon continues and is taking shape, transforming the Fort Gordon region into a cyberspace hub for the Army and the Nation.

Thanks to congressional support, Army talent management initiatives are also paying off. We will soon have the Army's first direct commissioned cyber officers, and our civilian cyber operators will have a new career management field. We are also incentivizing soldiers through expanded use of the assignment incentive pay and special duty assignment pay.

Partnerships remain critical to our efforts. We are leveraging the private sector, the academic community, and the key allies to rap-

idly develop and deliver new capabilities to the joint force and our Army.

In the future, the Army will require sustained investment in science and technology to capitalize on the advancements in artificial intelligence and other innovative capabilities. We also need to pursue force structure and capabilities at the Army corps level and below to ensure we have the tactical capabilities our pilot initiatives have shown.

Today, the Army is driving hard to lay the groundwork for the future force. With Congress' support, we will continue to build upon our momentum to deliver a formidable cyber force to our warfighting commanders.

Mr. Chairman, I would request my written testimony be entered into the official record, and I'm happy to answer the committee's questions.

[The prepared statement of General Nakasone follows:]

PREPARED STATEMENT BY LIEUTENANT GENERAL PAUL M. NAKASONE

Chairman Rounds, Ranking Member Nelson, and Members of the Subcommittee, I want to thank you for your continued support of U.S. Army Cyber Command (ARCYBER) and our efforts operationalizing cyberspace for the Army in support of our warfighting commanders. It's an honor for me to represent the extraordinary soldiers and Army civilians of ARCYBER and the entire Army Cyber Enterprise. My testimony focuses on the Army's ongoing progress and key milestones the Army has reached since I last testified before this subcommittee in May 2017.

Army Cyber Command's mission is to direct and conduct integrated electronic warfare, information and cyberspace operations as authorized, or directed, to ensure freedom of action in and through cyberspace and the information environment, and to deny the same to our adversaries. Our operational units include: the Joint Force Headquarters-Cyber (Army); the Network Enterprise Technology Command (NETCOM); the 780th Military Intelligence Brigade (Cyber); the 1st Information Operations Command; and the Army Cyber Protection Brigade.

To be successful in our challenging mission, we closely partner with the other members of the Army Cyber Enterprise, which include the Army Cyber Center of Excellence (Cyber COE); the Army Cyber Directorate within the Headquarters Department of the Army (DAMO–CY); and the Army Cyber Institute at West Point (ACI). Together, the Army Cyber Enterprise has made significant progress, operationally and institutionally, in preparing the Army for the future fight.

Operationally, ARCYBER achieved a significant milestone in September 2017 when all 41 Army Cyber Mission Force (CMF) teams became fully-operational, a year ahead of U.S. Cyber Command's (USCYBERCOM's) mandate. These teams were put on-mission as soon as they became available. In addition to these 41 Active component teams, the Army is building 21 Reserve component (RC) teams trained to the same Joint standards and integrated into a Total Force team. Last August, the first Army National Guard (ARNG) Cyber task force—Task Force Echo—assumed a critical mission for USCYBERCOM to engineer, install, operate, and maintain critical network infrastructure.

Today, the Army's Total Cyber Force is in the real-world fight 24/7—against near-peer adversaries, ISIS, and other global threats. Since last May, ARCYBER has provided support to Army commanders, with special emphasis on the Pacific theater, to ensure select networks, systems and data are protected and secure. Army cyber forces have also supported the Joint force as an integral part of Joint Task Force ARES (JTF–ARES), a JTF that I'm privileged to lead that has been countering ISIS' use of cyberspace as a domain to spread messages and coordinate combat activity. The work of JTF–ARES has been an important part of the coordinated multi-domain military campaign that helped defeat ISIS on the ground in Iraq and Syria.

Institutionally, the Army Cyber Center of Excellence has made significant progress developing the cyber workforce. In August, the first class of enlisted cyber operators graduated the Army Cyber School. The Cyber School is now training all soldier cohorts (officers, warrant officers, and enlisted members) from all three force components (Active, Guard, and Reserve). The first Reserve component soldiers graduated from the Cyber School in fiscal year 2017.

The Army invests approximately $1.9 billion annually to fund the cyber workforce, operational units, and operate and maintain the Army portion of the DOD information network (DODIN). Investments into our cyber capabilities remain a top priority and we are continually refining our requirements, and improving resourcing and acquisition processes to ensure that they are agile enough to rapidly translate innovative concepts into realized capabilities.

Building on the Army's operational and institutional momentum, ARCYBER has pursued three mutually supported priorities: aggressively operate and defend our networks, data, and weapons systems; deliver effects against our adversaries; and design, build, and deliver integrated capabilities for the future fight. The following narrative describes the Army Cyberspace Enterprise's accomplishments across these priorities encompassing the areas of Operations, Readiness, Resources, Training, and Partnering.

OPERATIONS

Cyberspace operations encompass three interrelated mission areas: Department of Defense Information Network (DODIN) operations, Defensive Cyberspace Operations (DCO), and Offensive Cyberspace Operations (OCO). Army DODIN operations, which include building, operating, defending, and maintaining the Army's portion of the DODIN, is our most complex mission because it underpins essential Army functions from mission command to business operations. Most cyberspace operations are defensive. Army Cyber Command's five Regional Cyber Centers (RCCs) provide enterprise-level defensive cyberspace operations and DODIN Operations support to our Network Enterprise Centers, including local information technology services. We are currently standardizing our RCCs to ensure effective and efficient alignment of missions, tasks, manning, structure, and tools. Additional efforts to improve our network defense include "Bug Bounty" exercises and the Vulnerability Disclosure Program that partners us with industry to use the best ethical hackers to identify and fix previously unknown vulnerabilities in Army networks.

The 20 Cyber Protection Teams (CPTs) of our Army Cyber Protection Brigade (CPB) conduct Active Defensive Cyberspace Operations and are invaluable in thwarting adversary actions that threaten critical Army and DOD networks and systems. Our CPTs deploy worldwide with mobile capabilities within hours of notification to protect and defend the Army's critical infrastructure, platforms, weapons systems, and data, supporting both national requirements and Joint and Army commanders.

Offensive Cyberspace Operations are cyberspace operations intended to project power by the application of force in or through cyberspace. The Army Cyber Mission Forces execute OCO using the same process of delegation of authority that governs conventional military combat operations, descending from the President, to the Secretary of Defense, to Combatant Commands and United States Cyber Command. The Army also has 21 OCO teams that are aligned in support of five Operational Commands: Cyber Command, Central Command, European Command, Pacific Command and Africa Command.

READINESS

Readiness is the Army's number one priority. Once Army Cyber Command (ARCYBER) completed the build of all 41 Army Active Component Cyber Mission Force (CMF) teams in September 2017, we transitioned from building cyber capacity to maintaining ready cyber forces. To do this, we are moving to a sustainable readiness model that will ensure our cyber forces are resilient and set conditions for multi-domain battle. Currently, we are investing $750 million into our Cyber Mission Forces.

To ensure our forces are ready to meet this challenge, the Army has funded a new cyberspace operations facility at Fort Gordon that will provide a cutting edge operational headquarters for both offensive and defensive operations. This facility is currently under construction, to be delivered in fiscal year 2020.

In addition to the proper facilities, ready cyber forces also require a firing platform, operational infrastructure, and access. To address these needs, the Army has built a rapid capability development network, and has adopted an operational platform that soldiers will use for training at the Cyber Center of Excellence and for operations upon graduation. Operational infrastructure provides the team's access to the cyberspace domain (Internet). A cyberspace capability is a device, computer program, or technique, including any combination of software, firmware, or hardware, designed to create an effect in or through cyberspace. The cyberspace capability is what enables the operator to create effects in and through cyberspace targeting specified systems or devices. The ability of a trained cyber team to bring each

of these technological capabilities to bear on a target is the true measure of readiness, and it is something that we are working every day to achieve.

ARCYBER is also working closely with the team developing the Persistent Cyber Training Environment (PCTE). When fielded, this system will provide an environment to train cyber operators both individually and collectively. The system will also be used to replicate various network environments that can be used to conduct mission rehearsals.

Sustainable readiness is not just focused on the Active component, it relies on the Total Army cyber force. The Army is building 21 Reserve component (RC) Cyber Mission Force teams, including 10 U.S. Army Reserve (USAR) teams and 11 Army National Guard (ARNG) teams, bringing the strength of the Total Army cyber force to 62 teams in total. These RC teams will be trained to the same Joint standard as the Active Duty Force.

Over the last 10 months, we have made progress closing gaps in timing, resourcing, and mission alignment to ensure these Army teams are effectively integrated into the DOD Cyber Mission Force (CMF). The ARNG is scheduled to have one CPT reach Initial Operational Capability in fiscal year 2018 and the USAR plans for two CPTs to reach Initial Operating Capability in fiscal year 2018. The Cyber COE continues to resource training for the RC teams, conducting transfer panels to transition existing soldiers into the Cyber branch as well as allocating seats for training at the Cyber School. Once the teams are manned, they will be fielded the same equipment as Active component teams. All 21 Reserve component CPTs will reach Initial Operating Capability by 30 September 2022 will be fully operational by 30 September 2024.

NETWORK READINESS

Network readiness is a critical component of overall Army readiness. We invest approximately $400 million annually into network readiness. The Army currently measures network compliance with policy, regulation, and law through the Cybersecurity Scorecard, Command Cyber Readiness Inspections (CCRI), and Command Cyber Operational Readiness Inspections (CCORI). To assist Army units in improving their network readiness, ARCYBER conducts staff assistance visits prior to inspections. During 2017, every organization that received a staff assistance visit improved their scorecard measurement by an average of 15 points during the CCRI. The number of unit networks that failed to pass a CCRI dropped from 23 to three. Thus far, in 2018, we have had no failures. Additionally, ARCYBER has placed a renewed emphasis and commitment on the integration of the ARNG networks.

Making our networks more defensible is the main thrust of our priority to, "aggressively operate and defend our networks, data, and weapons systems," designed to harden and modernize our networks and conduct defensive cyberspace operations. The Army is systematically improving its defensive posture with architecture modernization efforts that reduce attack surface area, improve bandwidth and reliability, and fortify our long-standing, but ever-critical perimeter defense capability.

A key priority has been upgrading Army computers to a more secure operating system, Windows 10 (WIN10). The Army recently achieved a major milestone with 95 percent of its approximately one million computers already upgraded. In order to stay ahead of the cyber threat, the Army is moving to an "as a service" approach for DODIN services and capabilities, while maintaining operational oversight. These efforts include endpoint management and security, Army Enterprise Data Centers, and cloud services.

Endpoint management security, network convergence, and cyber analytics are enhancing our situational awareness, enabling us to see and defend DOD networks and giving us unprecedented levels of DODIN/Defensive Cyberspace Operations integration to better enable the warfighter while defeating cyber threats. Big Data analytics are foundational to improving cyber readiness and resiliency. The Army is using data analytics to improve our situational understanding of our networks—to see not only adversary activity, but also ourselves; and using this information as part of a risk management strategy to inform our cybersecurity decision making. The Army is developing an analytic framework for conducting advanced cyber defense that begins with continuous monitoring of the cyber operational environment.

We are also continuing modernization efforts designed to improve the Army's ability to defend its networks; achieve greater standardization and interoperability; and dispose of older, less secure systems. Network modernization efforts include: Joint Regional Security Stack (JRSS) migration, Multiprotocol Label Switching (MPLS) upgrades, and Installation Campus Area Network (ICAN) upgrades.

Network modernization efforts are also allowing us to increase bandwidth significantly, critical to moving toward a cloud-based and virtualized architecture. In the

near future, the Army will use private, public, and hybrid clouds that will store and protect data in centralized repositories, improving data access and enabling global availability. As part of this effort, the Army is consolidating its data centers to enhance security and cost efficiencies. Reducing the Army's data center inventory will enable the follow-on transition to a long-term end state of four continental U.S. Army Enterprise Data Centers.

Additionally, as directed in the Section 1647 of the National Defense Authorization Act (NDAA) for fiscal year (FY) 2016, the Army's Cyberspace Operational Resiliency Assessment-Platform (CORA–P) program is evaluating the cyber vulnerabilities of major weapon systems. We are currently assessing 13 of 24 high priority systems. In response to Section 1650 of the NDAA for fiscal year 2017, the Army is developing a plan to evaluate cyber vulnerabilities in the critical infrastructure of 27 Army installations.

RESOURCES

The Army is on pace to man, train, and equip Total Army cyber forces to meet current and future threats. Readiness of the total force requires that our investments in cyber ensure that Active and Reserve forces are trained and equipped to common standards. People remain our most critical resource. Annually, ARCYBER spends $585 million to compensate its civilian workforce. Over the past 12 months we have devoted tremendous effort to ensure we can recruit, develop, employ and retain the talented workforce we need to accomplish our mission. We are also increasing our presence at key hiring fairs and participating in a number of existing internship programs. In addition, over the last three months we began exercising the direct hiring authority granted by Congress, which enables us to make on-the-spot tentative job offers at hiring fairs. All of these efforts should enable us to bring on hundreds of new civilian employees this year.

The Army has also begun conducting a Direct Commissioning pilot program, pursuant to the authority Congress gave us in Section 509 of the NDAA for fiscal year 2017, which will commission civilians directly into the Army as 1st Lieutenants. To date, over one hundred people have applied for direct commissioning, though unfortunately most have been unqualified based on age, education or experience. There are currently two candidates who will likely attend initial training in May 2018. Initial indications from the first two iterations of the Direct Commissioning pilot are that legal limits on constructive credit for cyber officers are preventing more qualified candidates from applying for the program.

Since I last testified, the Army has expanded two key compensation programs for cyber soldiers. Assignment Incentive Pay (AIP) is designed to encourage officers, warrant officers and enlisted soldiers to volunteer, train, and perform Cyber Mission Force work roles that are otherwise difficult to fill. Currently, ARCYBER has 1,850 eligible positions tied to AIP and the Army has budgeted approximately $1.6 million annually to compensate soldiers who fill those roles.

Special Duty Assignment Pay (SDAP) is designed to compensate enlisted soldiers assigned to duties designated as extremely difficult or that involve an unusual degree of military skill. Currently, ARCYBER has 1,245 eligible enlisted soldier positions tied to SDAP and the Army has budgeted approximately $108k annually to compensate those soldiers. Both programs will incentivize soldiers for the unique talents and skill sets that are required to execute the Army's overall cyber mission, and improve the readiness of the Cyber Mission Force.

In addition to monetary compensation, the Army also offers cyber soldiers the opportunity to participate in Training With Industry (TWI), or attend graduate school through the Advanced Civil Schooling program. ARCYBER also has the flexibility to detail some of our talented staff to the Defense Digital Service. These opportunities enable our soldiers to learn from industry, improve their education, and address some of the Department's toughest technological problems.

ARCYBER MOVE TO FORT GORDON, GEORGIA

Today, ARCYBER headquarters is split-based at Fort Belvoir, Virginia; Fort Meade, Maryland; and Fort Gordon, Georgia. Within four years, the ARCYBER headquarters will consolidate at Fort Gordon. As our Command transitions to Fort Gordon, the $180 million construction projects for our state-of-the-art headquarters is well underway, thanks to Congressional support. The new facilities will support more than 1,300 cyber soldiers and civilian employees, and are projected to be ready for occupation in summer 2020. Army Cyber Command is expected to be fully operational at Fort Gordon by 2022. With the addition of the ARCYBER headquarters, the Augusta, Georgia region will become a center of gravity for U.S. Army cyber-

space operations, providing a unified and consolidated operational and institutional home.

LIMITED ACQUISITION AUTHORITY

Following the establishment of USCYBERCOM and ARCYBER, both DOD and the Army recognized the need to find creative ways to maintain a competitive advantage in cyberspace. As it became apparent that speed and agility were critical in cyberspace, the Army needed to reduce the time and cost necessary to buy, test, and field new platforms and application technologies through the normal acquisition process. The Army subsequently initiated several innovative approaches designed to develop and deliver cyber capabilities more quickly, in order to keep ahead of our adversaries. This included granting ARCYBER Limited Acquisition Authority in August 2017, enabling us to meet the "need of speed" demanded in cyberspace operations. ARCYBER is using its Limited Acquisition Authority to wisely invest its resources in the most innovative and cutting-edge items that can rapidly benefit our force. We will likely leverage rapid contracting mechanisms such as Other Transaction Authority through partners like DIUx.

TRAINING

The Army Cyber Center of Excellence (Cyber COE) located at Fort Gordon, Georgia, provides training, force modernization, and career management for the Army's Cyber, Signal, and Electronic Warfare specialties. The Signal School provides trained soldiers to the operational force to conduct Department of Defense Information Network (DODIN) operations and cybersecurity. They train on average over 11,000 soldiers per year across 17 Military Occupational Specialties. Signal Soldiers install, operate, and maintain the Army's portion of the DODIN. The Signal School is aggressively pursuing a change to their training model that will provide all Signal Soldiers a common foundation in networking fundamentals in support of DODIN operations.

Established in 2014, the U.S. Army Cyber School trains Army Cyber Branch Soldiers and cyber personnel from the other Services. The Cyber School provides training in offensive cyberspace operations and defensive cyberspace operations at Fort Gordon, GA, and electronic warfare at Fort Sill, OK. The first class of Army Cyber Branch lieutenants graduated in May 2016; the first class of cyber warrant officers graduated in March 2017; and the first class of new cyber enlisted recruits graduated in August 2017. Additionally, the Cyber School has trained 101 sister Service personnel and 68 Army Civilians. The Cyber School trained a total of 151 Cyber Branch soldiers during fiscal year 2016 and another 305 soldiers during fiscal year 2017. The Cyber School has established all courses necessary to meet anticipated training requirements for over 900 soldiers annually to meet natural career progression and replacement of Cyber Branch Soldiers.

In addition to the Cyber School training, our Cyber Protection Brigade has developed "Cyber Gunnery Tables," similar in concept to the gunnery tables of maneuver branches, to ensure our Cyber Protection Team operators can effectively employ their DCO system. A Cyber Protection Team's DCO system enables the team to maneuver on Army networks to find, fix, and destroy enemy capabilities. These tables define the tasks that individuals, crews, and mission elements must master in order to effectively conduct DCO—Internal Defense Measures on the CPTs DCO system. They provide structured, methodical, and foundational training for individuals and teams. These gunnery tables also serve as training and readiness validation events, certifying that a crew has the required knowledge, skills, and abilities to participate in collective exercises as part of a mission element. They also provide a metrics-based assessment to objectively determine individual and crew readiness. Further, our teams use challenging competition-type exercises, such as Cyber Stakes, where individuals and teams can demonstrate their technical aptitude and sharpen their skills.

Additionally, the Cyber School is working several initiatives specifically directed at integrating Army Reserve component (RC) cyber forces. For example, in fiscal year 2017 the Cyber School conducted three Mobile Training Teams (MTTs) providing a total of 316 training seats; throughout fiscal year 2018 they will conduct seven MTTs, and they are prepared to support a minimum of seven MTTs in fiscal year 2019. These MTTs train approximately 30 students per iteration and are held at venues convenient to the Reserve component units. The Cyber COE has also conducted eight Cyber Branch Transfer/Reclassification panels and numerous off-cycle assessment panels for Reserve component applicants, selecting 470 soldiers from the Reserve component for transfer into the cyber branch. The Cyber COE is also working within the Army to ensure the Reserve component can build personnel capacity

and meet FOC training requirements without negatively impacting unit readiness reporting.

The Persistent Cyber Training Environment (PCTE) will provide high quality scenarios and event management to all four Services and USCYBERCOM, delivering a virtual environment that will enable training and mission rehearsals for squads, mission elements, and teams. The acquisition strategy for PCTE is to leverage existing infrastructure, transportation, and range resources, and to integrate the best government off-the-shelf and commercial off-the-shelf solutions. The program office is currently building cloud capacity that will host the Persistent Cyber Training Environment. Through incremental developments, the Army is creating low fidelity prototype training environments and leveraging the Service cyber components and DOD cyber ranges to develop high fidelity environments. Through a series of Cyber Innovation Challenges, two in progress to date, the program office will leverage industry and existing cyber training capabilities to refine event management and training management.

CSCB

Since 2015, the Army's Cyber Electro Magnetic Activities (CEMA) Support to Corps and Below (CSCB) pilot has been integrated into nine rotations at the Army's Combat Training Centers (CTCs), helping Brigade Combat Teams (BCTs) integrate CEMA, which spans offensive and defensive cyberspace, electronic warfare, and information operations into a BCT's operations process. This pilot has helped BCTs leverage CEMA to understand their unit's footprint in the cyberspace domain and in the electromagnetic spectrum, and to better deliver cyberspace effects and conduct electronic warfare in support of their operations. The pilot has also helped the BCTs to maximize the role of the organic Electronic Warfare Section and identified the best methods of leveraging the new Expeditionary CEMA Team concept under the proposed Cyberspace Warfare Support Battalion (CWSB).

The lessons learned through our CSCB initiative have been valuable and put to direct use. Today, our cyber forces are supporting operational units in Iraq, Syria, Afghanistan, Korea, and Europe. We're equipping and training units with new tools, giving them a marked advantage over the adversary. We're also supporting training for the new Security Force Assistance Brigade, providing expeditionary and remote OCO, DCO, Electronic Warfare, and Information Operations. ARCYBER is helping shape the CEMA capabilities of the Army's Multi-Domain Task Force initiative and lessons learned are being applied to global contingency operations. We continue to support the training of Brigade Combat Teams, helping build-out a contested and congested cyberspace domain and Electro Magnetic Spectrum infrastructure at Combat Training Centers and replicating real near-peer threats.

PARTNERING

In our headquarters we often say that cyber is a team sport. Since I last testified, we have partnered closely with the Defense Digital Service (DDS) on a number of important projects. We have worked closely with DDS to conduct a bug bounty on one of the Army's key logistics systems to identify and resolve vulnerabilities before our adversaries could find and exploit them. Additionally, we have partnered with them to pilot a new training program at the Cyber Center of Excellence for enlisted cyber soldiers. The intent of this pilot program is to shorten the training time for recruits. If recruits demonstrate the necessary skills, they can proceed more quickly through the training program. This more dynamic training format would enable many of the recruits with a computer science background to complete what was a six-month training program in as little as 12 weeks.

We have also partnered with the DDS to create tiger teams composed of DDS personnel and ARCYBER soldiers. One such team developed a counter-unmanned aircraft system (C–UAS) capability that can be used by battlefield commanders. Finally, Army Cyber Command has collaborated with DDS to develop an outpost at Fort Gordon, by the summer of 2018, which will facilitate identifying top technical talent to support the rapid development of solutions to top cyber threats.

Army Cyber Command is also closely partnered with Defense Innovation Unit—Experimental (DIUx). We meet monthly to share and collaborate on problem statements and commercial solutions that could address Army operational gaps and needs. Several projects sponsored by DIUx are under evaluation by ARCYBER for Defensive and Offensive Cyber Operations capabilities. In particular, we are assessing specialized software as a solution to endpoint threat detection/interrogation. We have also coordinated with DIUx for problem statements relating to Advanced Sensors and Machine Learning.

Key partners and allies bring unique capabilities, skills and approaches to the cyberspace operational environment. Each nation has benefited from our partnerships through information sharing and operational collaboration. Maintaining and improving these relationships will be critical to operational success regardless of the potential adversary.

CONCLUSION

The Army Cyber Enterprise has made significant progress throughout 2017.

- The Army's 41 Active Cyber Mission Force teams are fully operational, on-mission, and delivering unprecedented capabilities to our combatant and Army commanders every day.
- We are continuing to make our networks more secure and more defendable through modernization and consolidation.
- The Army Cyber Center of Excellence is now training all cohorts and all components, and preparing to integrate the Electronic Warfare force into the cyber career field.
- Construction on the Army Cyber headquarters complex at Fort Gordon, Georgia is taking shape, and will transform the Fort Gordon region into a cyberspace hub for the Army and the Nation.
- Our investments in soldiers and civilians through innovative talent management initiatives are paying off.

The Army is driving hard to lay the groundwork for the future force. We are moving toward developing a sustainable readiness model for the Total Army cyber force; building an in-house development capability; and organizing an expeditionary CEMA force. Every day our people are innovating and adapting, positively impacting the way we organize, train, and equip the Army cyber force, enabling us to stay ahead of our adversaries and to ensure the Army is ready to fight and win. With the continued support of Congress, the Army will continue to build upon this tremendous momentum to deliver an elite cyber force to our warfighting commanders.

Senator ROUNDS. Thank you. Thank you, Lieutenant General Nakasone.

All of your complete messages or reports will be entered into the record, without objection.

Vice Admiral Gilday.

STATEMENT OF VICE ADMIRAL MICHAEL M. GILDAY, USN, COMMANDER, UNITED STATES FLEET CYBER COMMAND, AND COMMANDER, UNITED STATES TENTH FLEET

Vice Admiral GILDAY. Chairman Rounds, Ranking Member Nelson, Senator Sasse, good afternoon. On behalf of the sailors and the civilians of Fleet Cyber Command, it's an honor to be here with my joint teammates, and I thank you for the opportunity to appear. I also want to thank you for your leadership and for your support in helping to keep our Nation secure in this complex domain of cyberspace.

Since appearing before this committee last year, and like my fellow cyber component commanders, I have continued to observe an upward trend in the capacity, the capabilities, the sophistication, and the persistence of cyberthreats against our networks. Cyberspace intersects every one of our Navy's missions, and it requires an adaptive approach to counter the threat.

Navy's approach for offensive and defensive cyber can really be summarized in three broad areas: first, modernizing our existing networks; second, by investing in new technologies and partnerships; and lastly, by carefully managing our talent.

First, we are modernizing and defending our networks by implementing our cyber resilience strategy, focused on hardening our network infrastructure and reducing its attack surface. We're in the fifth year of this ongoing effort. Further, we have extended our

defensive posture to include deploying defensive cyber teams with our carrier strike groups and our amphibious readiness groups.

Second, we are investing in new technologies and partnerships for the offense and the defense through a series of initiatives, including transitioning to cloud-based technologies. At the same time, we are investing in improvements to defend and to gain better situational awareness deep inside our networks. We are leveraging the data sciences through the Navy's new Digital Warfare Office, and collaborating with industry and academia to apply new technologies, like machine learning and artificial intelligence. We continue to mature partnerships with a host of allies and partners. We have established two new commands, one for doctrine development and the other for training, both improving the integration of cyberspace and electronic warfare into fleet operations.

Third, we're committed to growing and sustaining our talent base. Now that all 40 Navy cyber teams have reached full operational capability, we are focused, as Admiral—as General Nakasone said, on sustaining a mission-ready force. We are meeting, and in some cases exceeding, accession and retention goals for both officers and enlisted, as well as expanding our direct-commission cyber warrant officer and cyber warfare engineer programs to capitalize on our technical talent. We're improving the ways we integrate cyber talent from the Reserve force, and we are implementing the DOD's [Department of Defense] new Cyber Excepted Service Program for our civilian teammates. We are improving virtual training capabilities for all of our cyber teams, and we are building a new cyber center at the United States Naval Academy and offering graduate degrees for both officers and enlisted at the Naval Postgraduate School.

Lastly, I still believe we have much room to grow. In particular, we need to continue to seek improvements in how we recruit, how we train, how we retain, how we reward, how we fight, all the while ensuring that our forces are equipped to compete and defeat the adversary.

Mr. Chairman, Senators, thank you for the opportunity to be here this afternoon. I take the points from your opening remarks, and I look forward to answering your questions.

[The prepared statement of Admiral Gilday follows:]

PREPARED STATEMENT BY VICE ADMIRAL MICHAEL M. GILDAY

Chairman Rounds, Ranking Member Nelson and distinguished members of the Subcommittee, thank you for your continued support of the men and women of U.S. Fleet Cyber Command, U.S. Tenth Fleet, and the United States Navy. It is an honor and privilege to represent the outstanding sailors and civilians who comprise our U.S. Fleet Cyber/U.S. Tenth Fleet team, and I appreciate this opportunity to update you on how our Navy's cyberspace operations are evolving to remain competitive in today's strategic environment.

As discussed by the National Defense Strategy, great-power competition has re-emerged as the central challenge to U.S. security and prosperity. It will probably come as no surprise to this committee that our adversaries often act within the "gray zone," heavily relying on asymmetric methods such as cyberspace and information operations to undermine our national interests.

Over the past four years, as the Commander of U.S. Fleet Cyber Command and as the former Director of Operations for U.S. Cyber Command, I have observed first-hand how the United States is threatened by cyber-attacks every day; the threat to the U.S. Navy is certainly no different. Our ability to command and control our forces relies upon cyberspace. Virtually every operation aboard a Navy ship-naviga-

tion, engineering, communications and weapons employment—rests on the secure and reliable transfer of and confidence in our data. Operating in the maritime environment does not shield us from the threats inside of the cyberspace domain, and our competitors know this. The cyberspace domain is a great capability leveler due to the low cost of entry for adversaries who desire to achieve an effect against us. With interconnectedness and pervasiveness increasing due to the Internet of Things, this environment will only become more complex and contested.

Beyond today's threats, our current technological advantages are not preordained. We are in an unprecedented age of exponentially accelerating technology and a convergence of technologies that brings dynamic and innovative capabilities. The technological race is on for Artificial Intelligence, Machine Learning and Quantum Computing as the world's most powerful militaries strive to become the leader in these areas. Maintaining our role as a global superpower requires us to develop and evolve our cyber capabilities quickly to dominate in this technologically advanced environment.

In the same fashion that the historic U.S. Tenth Fleet from World War II enabled the prosecution of the U-Boat threat and ensured access to the shipping lanes of the Atlantic, U.S. Fleet Cyber Command and the modern U.S. Tenth Fleet exists today to enable, anticipate and prosecute cyberspace threats and ensure our Navy networks supporting our most critical missions are protected and ready.

Since its establishment on January 29, 2010, U.S. Fleet cyber Command [U.S. Tenth Fleet has grown into an operational force comprised of more than 16,000 Active Duty sailors, Reserve component sailors and civilians assigned to 29 Active Duty and 29 Reserve commands around the globe. U.S. Fleet Cyber Command reports directly to the Chief of Naval Operations as an Echelon II command and is responsible for operating and securing Navy Enterprise networks, defending all Navy networks, operating our global telecommunications architecture, and providing cryptology, signals intelligence (SIGINT), cyberspace, and space warfighting capabilities to support Fleet Commanders and Combatant Commanders. With distinct, but overlapping mission sets, U.S. Fleet Cyber Command serves as the Navy Component Command to U.S. Cyber Command for cyberspace operations, the Navy's Service Cryptologic Component Commander under the National Security Agency/ Central Security Service and the Navy's component for space under U.S. Strategic Command.

Headquartered in Fort Meade, Maryland., U.S. Fleet Cyber Command exercises operational control of globally-deployed Cyber Mission Forces (CMF) through a task force structure aligned to the U.S. Tenth Fleet. U.S. Fleet Cyber Command is also designated as the Joint Force Headquarters-Cyber aligned to U.S. Pacific Command and U.S. Southern Command for the development, oversight, planning and execution of full spectrum cyberspace operations aligned with other traditional warfighting lines of operations.

In 2015, U.S. Fleet Cyber Command released its Strategic Plan: 2015 to 2020, which identified five goals critical to deliver on our responsibilities by leveraging our strengths and shrinking the Navy's cyber-attack surface to cyber adversaries, which I will detail throughout this statement. Across the wide-ranging responsibilities, our five goals are:

1. Operate the Network as a Warfighting Platform: Defend Navy networks, communications and space systems, ensure availability and, when necessary, fight through them to achieve operational objectives.
2. Conduct Tailored Signals Intelligence: Meet the evolving SIGINT needs of Navy commands, including intelligence support to cyber.
3. Deliver Warfighting Effects Through Cyberspace: Advance our effects delivery capabilities to support a full spectrum of operations, including cyber, electromagnetic maneuver, and information operations.
4. Create Shared Cyber Situational Awareness: Create a shareable cyber common operating picture that evolves to full, immediate awareness of our network and everything that happens on it.
5. Establish and mature Navy's Cyber Mission Forces: Stand up 40 highly expert CMF Teams and plan for the sustainability of these teams over time.

We, the Navy and U.S. Fleet Cyber Command/U.S. Tenth Fleet, have made significant progress towards these goals, continue to develop organizationally and evolve to outpace competitors. On behalf of the warfighters of U.S. Fleet Cyber Command, I thank you again for opportunity to discuss the Navy's progress in cyberspace and our course ahead.

OPERATE THE NETWORK AS A WARFIGHTING PLATFORM

The Navy, like other DOD and government entities, faces enormous challenges in cyberspace. Foreign governments and non-state actors use cyberspace operations as an integral part of their national and military strategies. Adversaries take advantage of publicly available cyber tools so nefarious actors can quickly identify vulnerabilities in software and hardware to exploit high priority targets.

In May 2017, a cyber-attack known as WannaCry spread ransomware rapidly and indiscriminately across the world. The malware encrypted and rendered useless hundreds of thousands of computers in hospitals, schools, homes, and businesses in over 150 countries. In June 2017, numerous commercial ships transiting coastal waters in the Black Sea reported having their GPS systems "spoofed," so that their locations were reported inside Russian territorial waters, as opposed to being in international waters.

These examples demonstrate we operate in an increasingly contested cyber environment where information is the fuel of decision making and protecting that information and our mechanisms for Assured Command and Control (C2) are critical to successful maritime operations. Loss of this information, or lack of confidence in the veracity of the information we see, not only degrades our confidence and effectiveness of our C2, it also leads to loss of intellectual property and removes our competitive edge. The margins of victory are razor thin, and we cannot afford to lose a step.

U.S. Fleet Cyber Command/U.S. Tenth Fleet approach to overarching cyber defense is consistent with U.S. Fleet Forces Command's Fleet Design and the Chief of Naval Operation's plan for a Future Navy, with more innovation across the Fleet. The networks upon which the Navy depends to conduct its missions and fight effectively are presently under continuous probing, if not outright attack by determined adversaries. Simply put, any system with embedded information technology or networking capability is a target for an adversary. Technology is increasingly moving in the direction of everything defaulting to being networked so this environment will continue to increase in complexity and pose challenges to our operations.

U.S. Fleet Cyber Command directs operations to secure, operate, and defend Navy networks, which currently consists of more than 500,000 end user devices; an estimated 75,000 network devices (e.g., routers, servers); and approximately 45,000 applications and systems across multiple security enclaves. These systems are comprised of information technology, combat and operational technology and control systems. I can most succinctly capture our approach to cybersecurity by stating the Navy operates all of its networks as warfighting platforms. As a warfighting platform it must be aggressively defended from intrusion, exploitation and attack. As a warfighting platform, the network must be agile, resilient, and responsive to the C2, intelligence, logistics, and combat support functions that depend upon it. As a warfighting platform, its configuration must also be precisely maintained. It must be resilient to attack and allow us to "fight through the hurt." Finally, as a warfighting platform, it must be capable of and available to deliver warfighting effects in support of Combatant Commander operational priorities.

Reflective of the larger culture, the demand for seamless connectivity continues to grow, and solutions to visualize and protect this operational key terrain must keep pace. The Fleet must have trust and confidence in its networks, systems and data, and the information and knowledge they present. Failure to adequately protect and assure our Fleet networks would be detrimental to our maritime operational capability and warfighting effectiveness. Therefore, the importance of a secure architecture for Navy networks cannot be overemphasized. Our Systems Commands, Program Executive Offices (PEOs) and government research centers play a pivotal role in design and acquisition of our systems. Their focused R&D efforts of secure, resilient architectures and systems, reinforced by industry and academia best practices, are needed to ensure we are investing in the right systems, technologies and methodologies to provide a resilient information environment that can be operated and maintained by our personnel. Effective systems engineering also highlights the importance of ensuring our cybersecurity processes are intertwined with our network capabilities so we can maintain proper cybersecurity controls. Designing, developing, testing and fielding systems resilient to cyber exploitation is a key step in this. As the Navy Authorizing Official (NAO), we serve as a the oversight authority through utilization of the DOD Risk Management Framework to ensure new systems include the proper cybersecurity controls and identification of risk on our networks from design through fielding, and most importantly throughout their operating lifecycle.

Additionally, U.S. Fleet Cyber Command is operationally focused on continuously improving the Navy's cyber security posture through an emphasis on the combination of people, process and technology. This allows us to reduce the network intru-

sion attack surface, implement and operate layered defense in depth capabilities, and expand the Navy's cyberspace situational awareness as outlined below.

Reducing the network intrusion attack surface

Opportunities for malicious actors to gain access to our networks come from a variety of sources such as known and zero-day cyber security vulnerabilities, poor user behavior, and supply chain vulnerabilities. Operationally, we think of these opportunities in terms of the network intrusion attack surface presented to malicious cyber actors. The greater the size of the attack surface, the greater the risk to the Navy mission. The attack surface grows larger with aging operating systems and when security patches to known vulnerabilities cannot be rapidly deployed across our networks, systems, and applications.

The Navy is taking positive steps in each of these areas to reduce the network intrusion attack surface including enhanced cyber awareness training for all hands, enhancements to how we monitor our networks for compliance and vulnerabilities, reducing the time to field patches and fixes, and improving the process on how we inspect the cyber readiness of our networks.

An example of an innovative approach to reducing our attack surface is our Continuous Hardening and Monitoring Program (CHaMP) initiative. CHaMP brings together current and historical information from all sources, Navy attack surfaces and network operations to focus our network and operational system hardening and remediation efforts. The program aims to include continuous machine-assisted assessments of Navy commands' vulnerability management compliance, Information Assurance accreditation status, and network owner responsiveness in securing their networks. Based on threat indicators and command performance relative to Navy and DOD cybersecurity standards, the CHaMP program will be used to prioritize the assignment and deployment of our Navy Blue Team and other cybersecurity response activities.

Furthermore, we are bolstering our ability to manage cyber security risks in our networks by closely integrating our access and authorized activities with operations and risk-based inspections. This allows us greater understanding of IT challenges and configuration management processes. Through our work with industry partners and academia we are exploring ways to utilize data analytics, machine learning, and other automation technologies to do some of the cybersecurity heavy lifting that will bring our defensive posture to the next level.

Additionally, the Navy is reducing the attack surface with significant investments and consolidation of our ashore and afloat networks with modernization upgrades.

The Navy's Next Generation Enterprise Network-Recompete (NGEN–R) is an evolution building on the successes of the current ashore enterprise contracts (Navy Marine Corps Intranet and OCONUS Network (ONENET)). By incorporating lessons-learned from Operation Rolling Tide in 2013, a large-scale network maneuver and operation to eradicate an adversary from the Navy's unclassified network, and combining our overseas and CONUS shore enterprise networks under NGEN–R we can improve situational awareness, and our ability to C2, and operate and defend Navy networks. The enhanced situational awareness capability of NGEN–R will enable our headquarters and network defense forces to make better informed network operational decisions, and improve speed and agility to maneuver our networks for maximum effectiveness.

Often times, people are viewed as the largest vulnerability in this equation—by that same logic, our people, each and every person touching a keyboard, can make the network stronger. We believe a Navy cyber defense is an all hands effort like damage control on a ship. Our entire Navy needs cyber training but not everyone requires the same level of instruction. So we have developed tailored cyber training for our cyberspace workforce, leaders, average users and those who require escalated privileges. All Navy personnel are required to complete online cybersecurity awareness training upon hiring or accession, with an annual refresher. For the cyberspace workforce, the Navy is providing training that enables them to effectively conduct cyber offensive and defensive operations. Like other warfighting lines of operation? cyberspace operations training is also being delivered to an increasing number of officers via their professional military education, as well as in undergraduate and graduate school curriculum. The Navy addressed the need to integrate cyber training in other leadership development courses as well throughout the ranks. Finally, systems and operational commands identified enhanced users who require specialized cybersecurity training based on the roles they perform. For example, certain engineers at the systems commands will receive cybersecurity training so they are able to build better defend their unique networks and systems. Some of this training is already underway. An example of an operational enhanced user would be select shipboard technicians trained to recognize cyber threats to their

operational technology/industrial control systems and recover them from attacks against those systems.

Enhance our Defense in Depth Operations

The Navy is working closely with U.S. Cyber Command, NSA/CSS, our Cyber Service counterparts, DISA, Inter-Agency partners, and commercial cyber security providers to enhance our cyber defensive capabilities on all of our networks through layered sensors and countermeasures including the interface with the public internet on our unclassified networks down to the individual computers that make up our Navy networked environments. Key to this is our ability to detect and react to adversary activity and restore capability quickly. These defensive measures are informed by all source intelligence and industry cyber security products combined with knowledge gained from analysis of our own network sensor data. As information sharing improves, so does the shared responsibility for mutual defense.

From the long-haul communications that form our wide area network backbones to software and infrastructure purchased as a service such as commercial cloud, we are dependent upon commercial industry and share our cybersecurity responsibilities in partnership with them. While the rise of dual-use technology has created vulnerabilities, it has also created opportunities for us. Many of our challenges are not unique to the .mil domain and are shared by commercial industry. We fend off the same cast of adversaries, who are using the same tactics, techniques and procedures within .edu, .gov and .com domains. We work similarly to reduce the attack surface by applying countermeasures and patching known vulnerabilities on the same types of network infrastructure. Industry is and will remain a critical mission partner through technology development, sharing lessons learned, sharing risks, and responsible intelligence sharing.

As industry evolves capabilities we can employ, we include those in our overall architecture, and we are currently piloting and deploying new sensor capabilities to improve our ability to detect and respond to adversary activity as early as possible. In the future, we see industry advances in the fields of Artificial Intelligence (Al) and machine learning will allow us to continually improve the tools we employ on our networks to enable a more predictive and automated cyber defensive environment. It's a fast paced fight. We need to respond faster than the adversary and envision automation as the means to outpace the threat. This includes increasing the diversity of sensors on our networks, moving beyond strictly signature-based capabilities to behavioral sensing, and improving our ability to proactively detect new and unknown malware. We need these tools to help us sense what is "normal" and detect what activity on the network is just outside that, so we can act quickly. Capable adversaries will operate at or below the "noise level" so using the advanced analytics enabled by Al and machine learning will give us a tactical advantage in identifying malicious activity early. We are working with partners to investigate the best way to use these data science technologies for mission assurance.

At the tactical edge, 17 of our 20 Cyber Protection Teams are deployed around the globe today as well as five afloat Defensive Cyberspace Operations (DCO) teams deployed within our Carrier Strike Groups and Amphibious Ready Groups. We are leveraging big data analytics, as well as machine learning to improve our ability to protect that data in our networks. We also work closely with our Navy systems commands (SYSCOM) , such as Naval Sea Systems Command (NAVSEA), Naval Air Systems Command (NAVAIR), and Space and Naval Warfare Systems Command (SPAWAR), for example, in order to protect our weapon systems and platforms from cyber-attacks. Each of the Navy systems commands provides full life-cycle support for a specific category of military hardware or software, including research and development, design, procurement, testing, repair, and in-service engineering and logistics support. Our partnerships with the SYSCOMS help to expand our cyberspace situational awareness and protecting our assets effectively.

The Navy continues to support the spirit and intent of the Joint Information Environment (JIE), including the implementation of a Single Security Architecture (SSA) that begins with the Joint Regional Security Stacks (JRSS). The Navy and Marine Corps Intranet is our primary onramp into JIE, including incorporating JIE technical standards into the acquisition of the Navy Enterprise Networks as those standards are defined. In parallel, the Navy is setting internal technical standards for implementation of a Defense in Depth functional architecture across all our systems commands and networks, afloat and ashore—from standard desktop services to combat systems and industrial control systems. Additionally, the Navy is well into the transition along with the rest of DOD to the Risk Management Framework, which is drawn from a solid basis using National Institute of Standards and Technology practices. This is significant as it moves us from an antiquated compliance focus perspective to one of risk focus informed by intelligence, providing improved

cybersecurity, a concept we are applying to all of our networks IT, industrial controls and Combat Systems. Most importantly, we are integrating ways to better understand operational cybersecurity risk and defensive posture throughout an information system's life cycle. Operations in cyberspace are highly dynamic; we can only achieve a truly defensible architecture by investing in automation of the collection, integration, and presentation of data built in from the beginning as an integral part of each system. These actions will help us to truly build cybersecurity and resilience in initial system design and development and avoid the pitfalls associated with trying to bolt them on at the end. Continuous monitoring is critical to our understanding of how consistently our systems are properly configured in accordance with standards. Only then can operational commanders make cyber maneuver decisions with confidence that they will deliver the intended results.

JRSS will become part of our future defense in depth capabilities. As described above, the Navy has already consolidated our networks behind defensive sensors and countermeasures. We expect that JRSS v2.0 will be the first increment connected to the Navy Enterprise Networks. Accordingly, the Department of Navy is planning to consolidate under JRSS 2.0 as part of the technical refresh cycle for NMCI when JRSS meets or exceeds existing Navy capabilities. Integrating the Navy Enterprise Network with the JRSS will allow shared visibility into the boundary capabilities for Navy and DOD.

As we make improvements in our monitoring of Navy networks, we will continue to feed that operational picture into the JIE joint environment to ensure shared situational awareness across DOD of the Navy's portion of the Department of Defense Information Networks as a risk to one is shared by all.

For our part, U.S. Fleet Cyber Command is operationally focused on continuously improving the Navy's cyber security posture by reducing the network intrusion attack surface, implementing and operating layered defense in depth capabilities, and expanding the Navy's cyberspace situational awareness.

Create Cyber Situational Awareness

Just like any other domain, success in cyberspace requires awareness of both ourselves and our enemies. It requires that we constantly monitor and analyze Navy platforms within both the classic maritime system and global information system. The Navy continues down the acquisition path to expand our Navy Cyber Situational Awareness (NCSA) capabilities with a more robust, globally populated and mission-tailorable Cyber Common Operating Picture (COP). A new capability under development called SHARKCAGE will provide us significantly improved analytics and speed of response by leveraging the power of machine learning. In parallel, we are establishing the organizational linkages required giving context to that pictureand our data strategy focuses on seamless integration with all DOD network operations, industrial controls, and maritime operations data. For example, we are collaborating with Navy Facilities Command (NAVFAC) to include sensor feeds from industrial control systems into our NCSA, informing operators of the cyber defensive status of critical infrastructure systems for a more holistic view for mission assurance.

U.S. FLEET CYBER COMMAND OPERATIONAL FORCES

Status of the Cyber Mission Force

The CMF has three primary missions: Defend the nation against national level threats, support combatant commander missions, and defend Department of Defense information networks.

Navy teams are organized across existing U.S. Fleet Cyber Command operational commands at cryptologic centers, fleet concentration areas, and Fort Meade, depending upon their specific mission. Navy is responsible for sourcing four National Mission Teams, eight Combat Mission Teams, and 20 Cyber Protection Teams, and for their supporting teams consisting of three National Support Teams and five Combat Support Teams.

Given the dynamic nature of the cyber environment, our Navy CMF teams have achieved and must sustain a high degree of readiness. All 40 of the Navy-sourced CMF teams achieved Full Operational Capability (FOC) as of October 6th, 2017, one year ahead of the designated U.S. Cyber Command target. Navy CMF teams are currently actively engaged in cyber offensive and defensive operations globally as part of the joint force.

FOC is an externally validated evaluation indicating the unit has met all its capability requirements and can perform its mission as designed. However, it is not a measure of combat readiness. Achieving FOC was only a waypoint as the Navy's operational need for a well-trained and motivated cyber workforce will continue to

grow in the coming years. Although reaching this milestone is a great accomplishment, the true challenge is in sustaining that high degree of readiness and the ability to promptly 'answer all bells' when directed by U.S. Cyber Command. We are meeting that readiness challenge through continuous execution of current operations, a robust training program and in ensuring our forces have the tools and infrastructure they need to succeed.

Additionally, we have focused on the integration of our Fleet's efforts, capacity and capabilities across the Navy and Joint force. In my role as the Joint Force Headquarters-Cyber commander aligned to U.S. Pacific Command and U.S. Southern Command, this is an area where organizationally we have made significant progress last year.

Our planning with U.S. Pacific Command must be robust enough to create cyber support plans that are integrated into their operational plans in the more traditional warfighting areas. This requires a staff that is fully embedded into the supported combatant commander processes while being synchronized with my main staff at the Headquarters at Fort Meade. As a JFHQ–C Commander, I directed an extension of my staff in February 2017 to integrate at U.S. Pacific Command and provide cyberspace planning and force employment into operations alongside forces from the other warfighting domains. We organized our CMF teams, which included three U.S. Air Force CMF teams and two U.S. Army CMF teams, as well as my Navy CMF teams, in Hawaii to form an interim Cyber Forward Element as a one-stop-shop for full spectrum cyberspace operations in support of U.S. Pacific Command. This extension of my staff provides Offensive and Defensive Cyberspace planning to PACOM until a permanent Cyber Operations Integrated Planning Element, or CO–IPE, is in place. A CO–IPE, serves as the forward extensions of Joint Force Headquarters—DODIN and Joint Force Headquarters-Cyber. We are in the process of standing up three permanent CO–IPE at PACOM, SOUTHCOM and United States Forces Korea, working with our combatant commanders to project power in, from and through cyberspace. These Elements will also fully integrate cyberspace into battle plans, ensuring timing and tempo are set by the commanders for use of cyberspace effects in the field based on their operational scheme of maneuver.

Reserve Cyber Mission Forces

Through ongoing mission analysis of the Navy Total Force Integration Strategy, we developed a Reserve CMF Integration Strategy that takes advantage of our 298 Reserve sailors' skill sets and expertise to maximize the Reservist support for full spectrum cyber operations. These Reservists are being brought into service through fiscal year 2018, and will be individually aligned to Active Duty CMF teams and the Joint Force Headquarters-Cyber. In this way, we can employ the unique skillsets our Reserve sailors bring to the fight, while building a cadre of highly trained personnel that can be ready for surge efforts now and in the future.

As our Reserve cyber billets are fully manned and these personnel trained over the next few years, we will continue to assess our Reserve CMF Integration Strategy and adapt as necessary to develop and maintain an indispensably viable and sustainable Navy Reserve Force contribution to the CMF.

We are also exploring relationships with academia by establishing reserve detachments with high-performing academic research institutions. For example, this past year, we have directed and resourced the creation of a reserve detachment (FCC/C 1 OF Det Pittsburgh), attached to Navy Cyber Warfare Development Group (NCWDG), whose mission is to better leverage the research and technology rising out of Carnegie Mellon University (CMU) and Software Engineering Institute (SEI) in Pittsburgh, PA. This was initiated to better connect with advances in the academic world in order to enhance our cyber mission force training and cyber tool development.

Recruit and Retain

In fiscal years 2016 and 2017, the Navy met officer and enlisted cyber accession goals, and is on track to meet accession fiscal year 2018 goals in May of 2018. Currently authorized special and incentive pays, such as the Enlistment Bonus, should provide adequate stimulus to continue achieving enlisted accession mission, but the Navy will continue to evaluate their effectiveness as the cyber mission grows.

Today, Navy Cyber Mission Force (CMF) enlisted ratings (CTI, CTN, CTR, IS, IT) are meeting retention goals. Sailors in the most critical skill sets are eligible for Selective Reenlistment Bonus (SRB). SR–B contributes significantly to retaining our most talented sailors, but we must closely monitor its effectiveness as the civilian job market continues to improve and the demand for cyber professionals increases. Additionally, Navy is reviewing whether additional incentives for our most critical skill sets, such as Interactive On-Net Operators (IONs), are warranted.

Cyber-related officer communities are also meeting retention goals. While both Cryptologic Warfare (CW) and Information Professional (IP) communities experienced growth associated with increased cyber missions, we are retaining Officers in these communities at 93 percent overall. Both CW and IP are effectively-managing growth through direct accessions and through the lateral transfer process, thereby ensuring cyber-talented officers enter and continue to serve. Additionally, since 2011, the Navy has 40 Cyber Warfare Engineers (CWE) in the ranks, the Navy's direct commission program for experienced and highly talented cyber professionals.

Fortunately, the Navy has had seen a sufficient quantity and quality of individuals via our established accession means (USNA, ROTC, OCS, direct commissions, etc.) for CW, IP, CWE and Cyber Warrant Officers (CWO) communities. Leveraging special authorities granted by Congress as the time is not necessary (10 U.S. Code 533(g). However, as the "War for Talent" continues due to the combination of an upward trending economy and an ever increasing competition for cyber skillsets, this authority will allow the Navy to remain competitive in the future as necessary.

With respect to the civilian workforce, we currently have 91 civilian positions within the Cyber Mission Force. Forty-seven of these positions are filling various work-roles throughout the CMF and the remaining 44 are our Computer Scientists/ Tool Developers. Currently we have 27 of the 47 positions filled throughout CMF; we continue to recruit for our 44 Tool Developers and have made 17 selections to date, and have 12 personnel onboard. We are aggressively hiring to our civilian authorizations consistent with our operational needs. Our primary challenges in recruiting are the current compensation allowable and competition with industry and other DOD entities. With this in mind, we are currently offering various incentives to potential candidates which includes higher step (step 7) on the GS pay scale, 10 percent of salary as a one-time recruitment incentive, 10 percent of salary for relocation expenses, and several years of assistance in student loan payback (5K per year). Even with these incentives, we are not competitive with industry or the National Security Agency (NSA), and we intend to increase these incentives in the near future. Additionally, we are optimistic that the Cyber Excepted Service implementation (Phase II) will help in our recruitment efforts. We plan to use all of the authorities available to us and hire to our Cyber positions, to include our JFHQ–C and CO–IPE, as expeditiously as possible.

As the economy continues to improve, we expect to see more challenges in recruiting and retaining our cyber workforce.

Educate, Train, Maintain

The Navy currently manages, under the Executive Agent appointment of the Cryptologic Training System, the Joint Cyber Analysis Course, which provides basic initial accession (1000-level training) skillsets for Cyber operations used by all services, including acting as the accession school for the Navy's Cryptologic Technician Networks rate. Further, Cyber and Information Security knowledge in accession are maintained in training for the Information Systems Technology rate and recently added basics for the Intelligence Specialist accession path. Officers in Cryptologic Warfare and Information Professional designators receive Cyber and Information Security requirements.

As directed in the NDAA of fiscal year 2016 and in close consultation with U.S. Cyber Command, the Navy is on tracking towards to begin resourcing training for sailors assigned to its CMF in fiscal year 2019. As also outlined in the January 2017 Cyber Force Model Training Transition Plan for foundational (2000-level) training, the Navy is prepared to execute administrative oversight of designated cyber training curriculum in fiscal year 2019. Two-thousand-level training for Navy organic Information Systems Technicians providing Information Assurance and Network Security functions are in place through Navy channels. Similar training for Navy organic operational Network Defense personal is conducted on an individual basis with future plans to transition to a systematic approach.

U.S. Cyber Command mandates Joint Cyberspace Training and Certification Standards for the CMF, which encompass procedures, guidelines, and qualifications for individual and collective training. Most of the training today is delivered by U.S. Cyber Command and the National Security Agency (NSA) in a federated but integrated approach that utilizes existing schoolhouses and sharing of resources while sailors are in an operational status. Through the CFMTT plan with resourcing, the Services will transition to providing sailors that have already received foundational training. CMF training specifically involves 54 role-specific, intermediate through advanced training pipelines using a mix of nearly 100 Joint, NSA National Cryptologic School (NCS), and multi-Service courses to prepare officers, enlisted and civilians for their CMF work roles. These training events are not only aimed at the individual sailors, but also provide operational team certifications and sustainment

training. Once certified, our team training is maintained throughout the year via several key unit level exercise events which allow individuals and the collective team to demonstrate required skills against simulated adversaries. U.S. Fleet Cyber Command/U.S. Tenth Fleet augments the required U.S. Cyber Command training pipeline in two ways—online skills development and the provision of supplemental academics.

Using the DOD's Enterprise Cyber Range Environment (DECRE) resources, provided by the Joint Staff, U.S. Fleet Cyber Command utilizes Joint Information Operation Range nodes (JIOR) to connect CMF teams with ranges which are representative of shipboard networks. These networks are used as offensive and defensive mission rehearsal platforms and to augment individual training for various team workroles. U.S. Fleet Cyber Command has also invested in a web-based individual and collective training platform, using a commercial virtual environment, to augment the academic portions of the U.S. Cyber Command training pipeline with hands-on skills development. The Persistent Cyber Training Environment (PCTE), managed by the Department of the Army, is expected to incorporate similar distributed training methodologies in module-based systems. When necessary, teams seek out and receive additional training based on work roles or specific mission requirements.

From a formal educational perspective, to develop officers to succeed in the increasingly complex cyberspace environment, the Navy offers the following opportunities for cyber development:

- *USNA:* The U.S. Naval Academy offers introductory cyber courses for all freshman and juniors to baseline knowledge. Additionally, U.S. Naval Academy began a Cyber Operations major in the Fall of 2013. Furthermore, the Center for Cyber Security Studies harmonizes cyber efforts across the U.S. Naval Academy.
- *NROTC:* Our Naval Reserve Officer Training Corps' program maintains affiliations at 51 of the 180 NSA Centers of Academic Excellence at colleges around the country. Qualified and selected graduates can commission as Information Warfare Officers, Information Professional Officers, or Intelligence Officers within the Information Warfare Community.
- *NPS:* For graduate-level education, the Naval Postgraduate School offers several outstanding graduate degree programs that directly underpin cyberspace operations and greatly contribute to the development of officers and select enlisted personnel who have already earned a Bachelor's Degree. These degree programs include Electrical and Computer Engineering, Computer Science, Cyber Systems Operations, Network Warfare Operations and Technology, and a masters of Applied Cyberspace Operations.
- *NWC:* The Naval War College (NWC) is also incorporating cyber into its strategic and operational level war courses, at both intermediate and senior graduate-course levels. NWC also integrates strategic cyber research into focused Information Operations 10/Cybersecurity courses, hosts a Center for Cyber Conflict Studies (C3S) to support wider cyber integration across the College, and has placed special emphasis on Cyber in its war gaming role.

Together with U.S. Naval Information Forces, we will be realigning several of our operational commands to stand-up an Information Warfare Training Group (IWTG) later this month. This new command will advance IW readiness and warfighting capabilities, including Cyberspace Operations (CO), through training, assessments and certification assistance for Type Commanders in order to prepare afloat and shore activities to face the challenges of a dynamic threat environment.

Future Cyber Workforce Needs

The Navy's operational need for a well-trained and motivated cyber workforce (Active, Reserve and civilian) will continue to grow in the coming years. We continue to analyze the readiness of our Cyber Mission Force and will adjust recruiting tools, as required.

U.S. Fleet Cyber Command/U.S. Tenth Fleet is partnered with University of Maryland's "Center for the Advanced Study of Language" (CASL) in researching aptitude assessments for our cyber workforce. Cyber workforce screening and recruitment may be aided by the refinement and implementation of the Cyber Aptitude and Talent Assessment (CATA). The CATA will enhance screening and selection of the individuals best suited for specific work roles and assist with vectoring personnel into the work roles where they have the best probability of success, potentially reducing the training pipeline, minimizing attrition and delivering the most capable workforce. Assuming success with ongoing developmental efforts, we will work with stakeholders to identify logical injection points. (Recruiting, Universities, Service Academies, etc.).

Fleet Readiness

The Navy's 2019 budget continues to prioritize readiness alongside the investments necessary to sustain an advantage in advanced technologies and weapons systems. Ensuring the cyber resiliency of networks is part of maintaining the readiness of warfighting platforms.

The budget continues funding to train and equip the CMF, provides investments in Science and Technology and information assurance activities to strengthen our ability to defend the network. To maintain our advantage in advanced technologies and weapons, funding is provided for engineering to improve control points and boundary defense across Hull, Machinery & Electrical, Navigation and Combat Control Systems and for Cyber Situational Awareness.

The Navy requested accelerated funding for procurement of Cyber Protection Teams (CPT) field deployable computing and analysis capability called Deployable Mission Support Systems (DMSS) in PB18. The procurement and sustainment of 40 DMSS kits is required by Navy Cyber Protection Teams (CPT) to conduct intensive, computationally-heavy analysis when reach back capability is unavailable or bandwidth is limited. Without accelerated funding, this will reduce the number of full-capability DMSS kits available to Navy CPTs and delay the program schedule by over one year. Operationally, this will drive the need to share a limited number of DMSS kits for missions that may occur across the globe. The PB19 request builds upon this effort and will significantly improve operational defensive cyber capability and readiness. Our total inventory objective of sustained DMSS kits is 40, which is projected to occur by 2021.

The Navy is requesting increased investment in Defensive Cyber Operations forces' ability to detect adversary activities and analyze cyber-attacks against Maritime Cyber Key Terrain (CKT) and to integrate all-source intelligence and Navy data to assess adversary capabilities. The goal of these investments is to improve the Navy's capacity to deliver to Operational Commanders, cyber situational awareness at all layers of the IT infrastructure and provide a cyber COP at our Fleet Maritime Operations Centers.

Continued funding for training is necessary to ensure operator proficiency as Fleet systems are modernized and become more complex. I believe the Navy's ability to appropriately fund training of our operators in these new technologies will improve operational readiness.

Summary

The proliferation of cyber capabilities, coupled with new warfighting technologies, will increase the incidence of "gray zone" operations against our Nation and our Navy. Over the past year and a half, we have seen information become a weapon of choice amongst our competitors. We view the information environment to include the domains of space, cyberspace and the electromagnetic spectrum, all merged together as key in our ability to get in front of our adversaries to deny them operational advantages. That invisible battle space is an area that we must optimize to win in the future.

The opening rounds of the next conflict will likely be in cyberspace—the Navy must be ready to prevent wars as well as win them. Therefore, we will conduct operations in and through cyberspace, the electromagnetic spectrum and space to ensure Navy and Joint/Coalition freedom of action and decision superiority while denying the same to our adversaries. The Navy is closely aligned with U.S. Cyber Command, Combatant Commands, joint and interagency partners, and other Services to support a whole-of-government response to cyber threats. We will continue to succeed by leveraging our strengths and shrinking our vulnerabilities. We will win in these domains through commitment to excellence and by strengthening our alliances across the U.S. Government, Department of Defense, academia, industry, and with foreign partners.

Thank you again for this opportunity to update you on the great work being done by the men and women of U.S. Fleet Cyber Command, U.S. Tenth Fleet and the U.S. Navy. I look forward to working closely with members of the subcommittee on cybersecurity and appreciate your support of the cyber investments included in the Navy's 2019 budget request. I'm happy to take your questions.

Senator ROUNDS. Thank you, Vice Admiral Gilday.

Major General Reynolds.

STATEMENT OF MAJOR GENERAL LORETTA E. REYNOLDS, USMC, COMMANDER, MARINE FORCES CYBERSPACE COMMAND

Major General REYNOLDS. Good afternoon, Chairman Rounds, Ranking Member Nelson, Senator Sasse, and other members of the committee. On behalf of the marines, the civilians marines, and the families of the United States Marine Corps Forces Cyberspace Command, I want to thank you for your continued support, and I appreciate this opportunity to update you on the tremendous progress that we've made since I was last before you in May.

I'd like to highlight what our marines are doing in the cyberspace domain, and how we've shifted our focus from building the command to operationalizing, sustaining, and expanding capabilities in this new domain.

Chairman, at MARFORCYBER, I have organized operations along three lines of effort, and I will briefly highlight those for you today. I use this framework to organize my activities and to measure our progress.

So, my first priority is to secure, operate, and defend the Marine Corps Enterprise Network, the Marine Corps portion of the DOD [Department of Defense] Information Network. We have continued to expand our definition this year of the MCEN [Marine Corps Enterprise Network] by including all elements of the Marine Corps IP [Intellectual Property] space, which includes our many disparate networks that are owned and managed by different commands across the Marine Corps. To be more defensible, we've collapsed domains this year, we've expanded our enterprise view of the network through a common service desk, an endpoint, discovery, and we are now—as General Nakasone mentioned—we are also nearing completion of upgrade to WIN 10 across the Marine Corps. We've also experimented with additional acquisition methods and models like DIUx [Defense Innovation Unit-Experimental] that are more responsive to the changing threat. We're looking forward to employing Cyber Command acquisition authority, when it makes sense.

Moving forward and in response to the National Defense Strategy, we know we must be prepared to fight tonight, and we will build the objective network capable of fighting and winning against a peer adversary in a contested information environment. So, recognizing that our ability to command and control is our center of gravity, we are participating in efforts with the United States Marine Corps Service Headquarters to design and build a more defensible network architecture.

My second priority is fulfilling our responsibility to provide warfighting capabilities through the development of ready, capable cyberforces to United States Cyber Command. I am happy to report that, as of January of this year, ahead of schedule, all of our 13 teams have reached full operational capability and are employed against priority missions. Many of our marines have participated in planning or executing offensive and defensive missions against today's adversaries, and are informing tactics and procedures on a daily basis. We are increasing our proficiency every day.

Now, to increase readiness and retention, and to increase skills progression, sir, as you mentioned, the Marine Corps, just last week, announced the creation of our cyberspace occupational field.

The creation of the MOS [Military Occupational Specialty] will allow us to deliberately provide targeted incentives for recruiting and retention. For our civilian marines, we are leaning into hire and transition our workforce to the Cyber Excepted Service. As part of our integrated planning element build in support of Special Operations Command, we have hired civilians across the SOCOM enterprise who are providing cyber intelligence and planning support for joint cyber fires.

My third priority is to provide support to the Marine Corps as it works to operationalize the information environment. As you are aware, the Commandant has modified marine formations to build greater capability in the information environment under the Marine Corps operating concept, and we are building additional DCO [Deployable Cyber Force] forces inside the MAGTF [Marine Air-Ground Task Force], experimenting with tactical cyber, and sharing lessons on the integration of cyber with other fires and other information capabilities. As we continue to increase our capability and our capacity, we look forward to occupying our new operational headquarters on NSA's [National Security Agency] campus next month.

I want to again take the opportunity to thank Congress for the military construction funding that enabled the development of our new building. This building is much more than just administrative spaces. It will serve as a platform for training, command and control, planning, and execution.

I am incredibly proud of the strides that we have made in operationalizing cyberspace in support of the MAGTF and the joint warfighter since I was last before you in May.

Thank you, Mr. Chairman and members of the committee, for inviting me to testify before you today, and for the support that you and this committee have provided our marines and their families. I look forward to continuing the dialogue and to answer your questions today.

Thank you.

[The prepared statement of General Reynolds follows:]

PREPARED STATEMENT BY MAJOR GENERAL LORETTA E. REYNOLDS

Major General Reynolds was commissioned a Second Lieutenant in May 1986 upon graduating from the United States Naval Academy. Throughout her career she has served in a variety of command and staff billets in the operating forces. As a Lieutenant, she served as a Communications Watch Officer at the Base Communication Center, and later returned to the Division Communications Company where she served as a Communication Center Platoon Commander, Multichannel Platoon Commander, Operations Officer, and Radio Officer. As a Captain and Major, she served with Marine Wing Communications Squadron 18, 1st Marine Aircraft Wing Okinawa, Japan as a Detachment Alpha Executive Officer and Commanding Officer. She served with the Ninth Communication Battalion, 1st Surveillance, Reconnaissance, and Intelligence Group as the Assistant Operations Officer and Commanding Officer, Bravo Company. As a Lieutenant Colonel, she commanded Ninth Communication Battalion, I MEF and deployed in support of Operation Iraqi Freedom II in Fallujah, Iraq. As a Colonel, she commanded I MEF Headquarters Group and deployed the Group to Camp Leatherneck, Afghanistan in support of I MEF FWD/Regional Command Southwest in Helmand Province during Operation Enduring Freedom. She recently served as the Commanding General, Marine Corps Recruit Depot/Eastern Recruiting Region, Parris Island, SC.

In the Supporting Establishment, she has served as an Acquisition Project Officer at the Marine Corps Systems Command, Candidate Platoon Commander for Charlie Company, Officer Candidate School, Commanding Officer of Recruiting Station Har-

risburg, Pennsylvania, an Action Officer and Deputy Division Head for Strategic Plans Division, Command, Control, Communications, and Computers (C4) Department, Headquarters Marine Corps and as Division Chief (J6) at the Joint Staff in the Pentagon. Her most recent assignment was as the Principal Director (Asia & Pacific), Office of the Deputy Under Secretary of Defense (Asia & Pacific).

Her professional military education includes the United States Naval Academy, The Basic School, the Basic Communication Officer's Course, Command and Control Systems Course, the Navy War College and the Army War College. She has earned Masters Degrees from both the Naval War College and the Army War College.

Her personal decorations include the Defense Superior Service Medal, Legion of Merit, Bronze Star, Meritorious Service Medal (with gold star), the Navy, and Marine Corps Commendation Medal (with gold star).

INTRODUCTION

Chairman Rounds, Ranking Member Nelson, and distinguished members of this Committee, I thank you for inviting me here today to represent the Marines and civilian Marines of Marine Corps Forces Cyberspace Command (MARFORCYBER). I appreciate this opportunity to update you on the tremendous progress we have made since I was last before this committee in May, to highlight what your marines are doing in the cyberspace domain and how we have shifted our focus from building the command to operationalizing, sustaining, and expanding capabilities in this warfighting domain.

Our Commandant, General Neller, made clear in his Message to the Force 2018 that the Marine Corps must be prepared to fight in order to make it to the next conflict. This includes our ability to fight—and win—in the domain of cyberspace. Our adversaries will test our superiority across the domains of air, land, sea, and space, in the next conflict. They are testing us in cyberspace today. Understanding this, and consistent with our Commandant's guidance, we are developing the Marine Corps' cyber capacity at the tactical level of war, so that in the future the Marine Corps will more effectively preserve the ability to fight and win in a contested environment and deliver effects in cyberspace.

It gives me great pride to share with you today the many accomplishments of the Marines and civilian Marines of MARFORCYBER, and the work they are doing to defend our nation from a growing and evolving threat.

MISSION AND ORGANIZATION

As the Marine Corps Service component to U.S. Cyber Command, MARFORCYBER conducts full spectrum cyberspace operations. This includes securing, operating and defending the Marine Corps Enterprise Network (MCEN), executing DOD Information Networks (DODIN) operations, conducting Defensive Cyberspace Operations (DCO) within the MCEN and Joint Force networks, and when directed, conducting Offensive Cyberspace Operations (OCO) in support of Joint and Coalition Forces. We do this to enable freedom of action in cyberspace and across all warfighting domains, and to deny the same to our adversaries.

As the Commander, MARFORCYBER, I wear two hats. I am Commander, MARFORCYBER, and I am the Commander of Joint Force Headquarters—Cyber (JFHQ–C) Marines. In these roles, I command about 1700 Marines, civilian Marines, and contractors across our headquarters and subordinate units. MARFORCYBER is comprised of a headquarters organization, a JFHQ–C, and two colonel led subordinate commands: Marine Corps Cyberspace Warfare Group (MCCYWG) and Marine Corps Cyberspace Operations Group (MCCOG). Through the JFHQ–C construct, we provide direct cyber operations support to U.S. Special Operations Command (USSOCOM).

In order to accomplish our mission, I organize operations along three lines of effort that I will highlight for you today. I use this framework to organize activities, allocate resources, grow capability, and measure our progress.

SECURE, OPERATE, AND DEFEND THE MCEN

My first priority is to secure, operate, and defend the Marine Corps' portion of the DODIN, the MCEN. We have continued to expand our definition of the MCEN by including all elements of the Commandant of the Marine Corps' IP space, which includes our many disparate networks that are owned and managed by different commands across the Marine Corps.

We accomplish this mainly through one of the two subordinate commands mentioned previously—the MCCOG. The MCCOG is responsible for directing global network operations and computer network defense of the MCEN. It executes DODIN Operations and DCO in order to assure freedom of action in cyberspace and across

warfighting domains, while denying the efforts of adversaries to degrade or disrupt our command and control.

With the increasing pace of operations in the cyberspace domain, the MCCOG, our primary DODIN and Cyber Security Services Provider (CSSP), was designated an operational Command in December 2016. Internally, the MCCOG is re-organizing to more effectively fight in a high tempo environment and to better align to its operational command designation. Their reorganization will be complete this April.

Simultaneous with its designation, in August 2017, the MCCOG stood a Defense Information Systems Agency (DISA) mandated Command Cyber Readiness Inspection (CCRI) and a pilot Command Cyber Operational Readiness Inspection (CCORI), successfully passing both inspections and maintaining its certification as the Marine Corps' only CSSP. Additionally, during this same timeframe, MCCOG's Marine Corps Information Assurance Red Team (MCIART), the team responsible for assuming an adversarial role and testing our layered defenses across the Marine Corps, was recertified by the National Security Agency (NSA).

The Marine Corps views the MCEN as a warfighting platform, which we must aggressively defend from intrusion, exploitation, and attack. Recent real-world defensive cyberspace operations have informed and sharpened our ability to detect and eliminate threats on the MCEN. The operational posture to address vulnerabilities is critical as exploits are identified by USCYBERCOM or through adversary action. Recent operational successes include the replacement of more than 200 Virtual Private Network (VPN) Devices across more than 120 distinct sites in less than a 90 day period. In addition, recent real-world operations, such as responding to destructive and malicious global ransomware (WannaCry) and wiperware (Petya/NotPetya) events, have improved our ability to aggressively and successfully compress patching timelines and enhance our defenses in order to avoid exploitation.

While the MCCOG maintains a persistent capability to defend the Marine Corps' cyber battlespace, MARFORCYBER is continuously seeking methods to enhance the Service's defenses. Beginning in December, MARFORCYBER began augmenting the MCCOG's capability with other rapid and persistent defensive cyber resources that can quickly identify a threat, defend an area, eject adversaries, and recover from malicious activity. Though actively engaging an adversary in our battlespace is critical, securing the battlespace from attack is our first line of defense. Understanding this, we have adopted a philosophy of ruthless compliance with security measures across all elements of the MCEN. We are using every security action to increase our partnerships with other MARFORs and major subordinate commands to exercise command and control, and increase their understanding of the constant threat our adversaries pose in cyberspace. Cybersecurity is a team effort and it requires everyone to be engaged. We rely on the buy-in from our partners to ensure that the MCEN is properly protected.

We have improved network visibility and security by consolidating our legacy systems into a single homogeneous network. Consolidating domains reduces attack surfaces and improves our ability to identify and respond to threats. We are aggressively consolidating legacy domains, transitioning to the WIN 10—operating system, and collapsing regional service desks to a single enterprise service desk. Our updates to each of these priorities are described briefly below.

Enterprise Service Desk. Since May, MARFORCYBER has been replacing regional service desks with a centralized, standardized Enterprise Service Desk (ESD) in Kansas City, Missouri to manage and monitor the MCEN, provide valuable insight regarding network trends, and rapidly respond to warfighter needs. The ESD is under the operational control of MARFORCYBER. While consolidation is not yet complete, the ESD has provided the anticipated benefits of improved service and network visibility, complementing other defensive actions on the MCEN. Our next step is to establish the Alternate ESD in New Orleans, and procure the equipment for both ESD locations. The fiscal year 2019 President's Budget requests the funding to continue to stand up the ESD.

Domain Consolidation and Elimination (DC&E). We are continue efforts to collapse legacy networks into a single, homogenous and secure network. Legacy networks increase the Marine Corps' cyber footprint and unnecessarily increase attack surfaces for adversaries. Eliminating these networks and consolidating them within the MCEN will provide much needed standardization, increase network visibility, and decrease the attack surface available to our adversaries. Out of 52 legacy domains, only 18 remain to be decommissioned. The largest program of record requiring migration is the Marine Corps Enterprise Information Technology Services (MCEITS), a system that provides collaboration, data exchange, and information access. Planning is underway to migrate MCIETS onto MCEN–N. We anticipate completing our DC&E efforts by September of 2019 however, additional actions are required to consolidate legacy networks onto the MCEN such as migrating public-fac-

ing webservers into demilitarized zones, consolidating data centers, and conducting Enterprise Infrastructure Modernization (EIM).

We are also participating in joint efforts to secure our networks, most notably by integrating into the Join Information Environment (JIE). Through JIE, the Marine Corps will install Multiprotocol Label Switching as part of the Joint Regional Security Stack (JRSS) project and will standardize transport while improving security. In addition, the Marine Corps continues working with Joint Force Headquarters—— DOD Information Networks (JFHQ–DODIN) to modernize infrastructure and comply with standards that protect our public-facing systems to reduce unnecessary and outdated public facing system, and harden and PKI-enable the remaining. Upgrades to the equipment and standards that safeguard our public-facing websites are underway to ensure we remain connected to the general public and industry while maintaining the latest in cybersecurity protections.

Windows 10. The Marine Corps continues its efforts to transition its Microsoft Windows end user devices to the Windows 10 (WIN 10) operating system (OS), effecting well over 100,000 devices on the unclassified network alone. In order to accomplish this task, MARFORCYBER exercised command and control relationships with Tier III Commanders and MARFORs to synchronize effort and resources, engage commanders across the force, and track progress. The Service leadership has supported our efforts; and we have been providing periodic updates on progress and compliance to the Assistant Commandant of the Marine Corps. Our WIN 10 transition is currently on plan to meet 31 March deadline established by DOD.

Cyber is a dynamic, competitive environment, and we are continually responding to the increasing capability and capacity of our adversaries. We are improving our ability to understand system data and identify vulnerabilities. Through participation in various joint exercises, we continuously affirm that treating cyberspace as a contested warfighting domain is essential to our ability to rapidly identify and defeat an adversary. During Exercise Pacific Sentry, a bilateral exercise led by U.S. Pacific Command and linked to U.S. Strategic Command and USCYBERCOM headquarters' exercises, we identified several key stakeholders and owners of Marine Corps information repositories who must aggressively defend themselves in cyberspace in order to provide essential, service level activities. Our experience during real-world operations and training exercises has demonstrated that many commands and processes within the Service that have historically been considered administrative in nature must operationalize in order to function in a contested cyberspace domain. For example, our partners in cybersecurity inside the Service include acquisition commands and data owners. In cyberspace, the Supporting Establishment must respond with the same readiness and agility as the warfighting element.

Moving forward, and in response to the National Defense Strategy, we must build the objective network capable of fighting and winning against a peer adversary. We are participating in efforts to shape our battlespace within the Service by designing a more defensible architecture. The Objective Network is a service-level capability that spans all war-fighting functions and enables operations across all domains. The Objective Network must be deployable and resilient to support command and control functions throughout the Marine Air Ground Task Force (MAGTF) in a contested, disconnected, intermittent, and low bandwidth environment. To operate in this environment, the network must adapt to conditions and optimize performance, while reducing detection and vulnerabilities.

The objective network is essential to "make sense" of the cognitive domain, where enterprise and local resources feed critical thinking to drive commander's decision-making and enable information operations. Artificial Intelligence (Al) is the core element in accomplishing this in near-real time. An interconnected family of MAGTF Al systems share priorities, monitor the network, learn patterns, and inform human decision making. This enables Al to manage hardware and software components, route network traffic, and reduce the electromagnetic footprint. The result is a resilient command and control network that supports the warfighter even in the most austere environments.

PROVIDE A CYBERSPACE WARFIGHTING CAPABILITY

My second priority supports our responsibility to provide ready, capable cyber forces to USCYBERCOM's cyber Mission Force.

The Marine Corps is responsible for 13 of USCYBERCOM's 133 Cyber Mission Force (CMF) teams: one National Mission Team (NMT), eight Cyber Protection Teams (CPTs), three Combat Mission Teams (CMT), and one Cyber Support Team (CST). These 13 teams are aligned against USCYBERCOM (Cyber National Mission Force), USSOCOM, and Marine corps missions.

Three of the eight CPTs are service retained and oriented to service missions, (23 percent of the total Marine corps CMF).

I am happy to report that, as of January 2018 and ahead of schedule, all of our 13 teams have reached FOC. All teams are fully engaged in supporting the mission. Although we have met FOC criteria, our work is not done. We have shifted our focus toward sustaining and improving our team readiness.

To increase readiness, improve effectiveness, and address retention of cyberspace operators, the Marine Corps recently established a Cyberspace Occupational Field. We have learned a great deal in the past several years about the training, clearance, and experience requirements across the cyber mission force. We know that in order to be effective, we must retain a professional cadre of cyberspace warriors who are skilled in critical work roles, and we know that many of our marines desired to remain part of the cyber work force. We intend to begin assigning marines to the cyberspace MOS on 1 October 2018. This will significantly improve both readiness and retention of the cyber force, and allow us to develop their skills throughout their careers.

I would like to thank Congress for authorizing the Marine Corps to grow its structure by 1,000 earlier this year to 185,000. Our growth in cyber is consistent with the Commandant of the Marine Corps' request to expand our ability to operate in the Information Environment and build capabilities that allow the Marine Corps' to increase its emphasis on maneuver in a cognitive sense, expanding our employment of combined arms to the domains of cyberspace.

The MCCYWG is our colonel led command that is responsible for identifying capability requirements, training, certifying, and sustaining readiness for our CMF teams. While they are currently minimally staffed, my vision for this command is to develop it into the centerpiece for advanced cyber warfare training, tactics, and certifications to support Marine Corps cyber forces. The Commandant of the Marine Corps recently approved growth for the MCCYWG to enable this vision in support ofjoint CMF and Marine Corps cyber units.

While building the CMF, members of the MARFORCYBER staff were dual-hatted as the Joint Force Headquarters staff. This year, the increasing pace of cyberspace operations demanded that we resource a separate, standing JFHQ–C. This JFHQ–C provides planning, targeting, and intelligence support to supported commanders, synchronizes execution of cyberspace operations, and provides command and control for CMTs and CST.

In May I updated you regarding the development of the Joint Force Headquarters—Forward, which was intended to integrate cyberspace operations with USSOCOM's global operations. Since then, the Secretary of Defense, through USCYBERCOM, instructed all Service Cyber Components to rename this organization the Cyberspace Operations—Integrated Planning Element (CO–IPE) and to complete an implementation plan no later than March of this year. We have been working through both USCYBERCOM and USSOCOM to identify and satisfy requirements in the most efficient manner possible.

In addition to the five marines already at USSOCOM headquarters, we begun to build the COIPE across USSOCOM organizations worldwide and look to complete the civilian hiring for a total 26 civilians by October of this year. We have also been working within the Service to increase our uniformed CO–IPE staff, with an increase of 13 marines required to meet our staffing goal by the end of fiscal year 2020.

As with all other domains, the marines continue to be "First to Fight" in cyberspace. Our CMTs working in support of Joint Task Force Ares have conducted multiple, large-scale operations to support U.S. Central Command (USCENTCOM) and Combined Joint Task Force—Operation Inherent Resolve. We have also expanded our support beyond the CMTs to include cyberspace operations planners working at multiple locations both overseas and here at home with partner organizations. I currently have numerous marines deployed to locations in both USCENTCOM and USAFRICOM, planning and integrating cyberspace operations into ongoing activities. We are also working within the Service to integrate cyberspace effects and planning into other domains. We recently deployed a Marine cyberspace planner to Afghanistan to assist the marines in Helmand Province as Task Force South West executes their advise and assist mission with our Afghan partners. Through my deployed personnel, we are bringing cyberspace operations to the tactical edge of battle, while at the same time generating cyberspace experience and expertise within operational units outside of USCYBERCOM. These experiences will allow operational planners to adapt the emerging cyberspace capabilities in such a way that we can incorporate cyberspace operations at all levels of conflict across the full range of military operations.

We continue to improve on the Marine Corps' investment in specialized tools for defensive cyberspace operations. The Deployable Mission Support System (DMSS) hardware and software tools comprise the weapons system CPTs use to meet any mission they may be assigned, from readiness and compliance visits to incident response or Quick Reaction Force missions. The DMSS toolkit evolves with the threat and is continually revised and upgraded to ensure CPTs have the most up-to-date toolkit available for a dynamic cyberspace operations mission set. MARFORCYBER is also working to develop a DMSS-like toolkit for employment by the Service's Defensive Cyber Operations—Internal Defensive Maneuver (DCO–IDM) Companies, which will provide an organic defensive cyberspace capability to Marine Expeditionary Force (MEF) Commanders within the newly established MEF Information Groups (MIG). MARFORCYBER is currently finalizing the engineering and procurement of third generation DMSS 3.0 kits, the first of which is scheduled to be delivered in late fiscal year 2018. Revisions in version 3.0 include: reduction in overall size of the system to allow for increased transportability on commercial flights, updated suite configuration to allow for split-based operations, leveraging reach-back capability to shared resources at a central location. We are working within the budget to address associated sustainment and operational support infrastructure.

We have established relevant operational capability in support of the warfighter and continue to experience consistent growth in operational capability and ability to deliver cyberspace effects.

OPERATIONALIZE THE INFORMATION ENVIRONMENT

My third priority is to add cyberspace warfighting expertise to the MAGTF and to enable operations in the Information Environment. Since our establishment in 2009, our marines and civilians have implicitly understood the need to provide a high return on the Marine Corps' investment in cyber.

The Marine Corps Operating Concept (MOC) describes a future operating environment where marines will fight with and for information, engage in a battle of signatures and be required to maneuver throughout networks even as we design networks that are maneuverable themselves. Last year, the Marine Corps developed a new force design to meet the needs of the MOC. This effort, called Force 2025, includes a DCO–IDM company and electronic warfare company for each MEF within the MIG. The DCO companies will provide MAGTF commanders with a trained and organized capability to conduct activities as maneuver elements for deployed networks, data stores and weapons system. As an element of the aforementioned MEF Information Group (MIG), the DCO–IDM Companies will support the defense of MAGTF key terrain in cyberspace and maintain a commander's ability to command and control. Their primary function will be mission assurance actions such, as actively hunting for advanced internal threats that evade routine security measures, performing incident response actions, and performing digital forensics.

MARFORCYBER continues to lead the DCO–IDM Training Pilot Program, which will inform the DCO–IDM Company concept of employment. We recently hosted DCO–IDM Training at MARFORCYBER, which included command leadership from all three MIGs as well as members of the DCO–IDM Companies. The pilot training included hands on training for the marines of the DCO–IDM Companies provided by MCCWYG as well as training for MIG leadership on employment, authorities, capabilities, and command and control. In addition, our Service retained CPTs remain engaged with the DCO–IDM Companies and continue to provide training opportunities. Members of DCO–IDM Companies have accompanied our Service CPTs during real-world operations and this partnership continues today.

To increase cyber readiness across the Service, we continue to emphasize the role of the Commander in the security and defense of the MCEN, and are conducting Cyber Readiness Visits at commands throughout the Marine Corps to identify cyber key terrain, assess readiness and culture, and bolster our defenses. As the Marine Corps' cyber career field comes online, we will aggressively build cyber operators to ensure the MAGTFs, bases and stations have the expertise and capacity to enhance cyber readiness not only at MARFORCYBER, but across the Marine Corps.

We have accomplished much in a short period working within the construct of these lines of effort, but still much work to do.

CYBER WORKFORCE MANAGEMENT

Since my last testimony in May, Headquarters, Marine Corps has approved my request to grow MARFORCYBER capability and capacity. We are now working on implementation as we nearly double the size of the command, adding more than 500 additional personnel, both uniformed and civilian. This growth includes increased capacity at the MARFORCYBER Headquarters staff, increasing the size of

MCCWYG to focus on improving our readiness through improved training and application of lessons learned across the Marine Corps, and creating a fully staffed JFHQ–C. This growth is programmed to occur over the next 5 years, starting this year and ending in fiscal year 2022. Our growth is in-line with the Commandant's vision and Future Force 2025.

At MARFORCYBER we have more than 60 reservists integrated into the command, both as mobilized marines who are working 365 days a year to support our mission, along with part time drilling marines who come in periodically over the course of the year for both individual training periods and two week Active Duty training periods. Both groups of reservists provide one of the three functions; MARFORCYBER staff augmentation, support to MCCYWG, and support to joint, academic, and experimental activities. Over the last year our Marine reservist have made numerous contributions, including filling key roles in the MARFORCYBER staff, as well as augmenting USCYBERCOM in support of operational requirements. The Marines providing Reserve support to the MCCYWG leverage skills they have acquired both in Service and from their civilian work environments. They support and augment CPT activities based on identified skill gaps. Recently, one of our CPTs had a scheduled mission and a last minute personnel gap was identified, and with 48 hours, a Reservist with the requisite skills volunteered to support the mission. This is just one example of how our Reserve marines are a force multiplier in the defense of the MCEN.

Marine Forces Reserve (MARFORRES), in conjunction with the current effort to increase Active Component (AC) DCO capability and capacity, is developing a Reserve component capability to augment, reinforce, and sustain AC MEF DCO requirements. The primary capability will be the activation and phased build of two Selected Marine Corps Reserve (SMCR) DCO–IDM Companies. These companies will be structurally similar to their AC counter-part companies and will most often be deployed and employed at the team level. MARFORRES' vision is to create meaningful opportunities for the population of marines who leave Active service, and to capitalize on their success and credentialing as civilians in the IT sector.

On the civilian side, the Office of Personnel and Management approved an increase in MARFORCYBER's recruitment and retention incentives from 25 percent to 50 percent. These additional incentives have assisted in hiring and maintaining critical cybersecurity civilian billets within MARFORCYBER. This increase provides us the ability to negotiate with the workforce, gaining ground against the private sector's ability to offer more money and incentives. In addition, we are participating in the DOD's Cyber Excepted Service (CES) Personnel System. The CES is a personnel system aligned to both Title 10 and Title 5 provisions that support the human capital lifecycle for civilian employees engaged in or in support of cyber-related missions. The implementation of this new personnel system will occur over three phases, with Phase II beginning in January of this year for the Service Cyber Components and, extending over a two year implementation process.

Policy that limits the recruitment of recently retired or separated service members that are cleared and fully trained has become substantially more difficult after the expiration of the policy suspending the 180-day cooling off period required before taking a government position. While there is a waiver process for uniquely qualified candidates, we have found that the waiver process itself is cumbersome and not timely, approaching 180 days in many cases. We are working with key stakeholders to help streamline the waiver process, which would help decrease the wait time in getting qualified personnel on board. To ensure that we are not unnecessarily losing our homegrown talent, the cyber workforce should be waived from this requirement.

As we continue to increase our capability and capacity, we look forward to occupying our new headquarters building on NSA's campus. I want to again take the opportunity to thank you for the Military Construction funding that enabled the development of our new headquarters. When I was last before you in May, I updated you on the development of this new operational headquarters facility, designed to meet the demands of our increased mission. Previously referred to as the East Campus Building—Marine Corps, I am pleased to inform you that we have received approval from within the Service and USCYBERCOM to name our new facility after an American hero, Colonel Alva B. Lasswell. Colonel Lasswell was a World War II cryptologist credited with translating an intercepted message that revealed Japan's planned attack on Midway Island. Colonel Lasswell's work enabled Admiral Nimitz to appropriately plan history's first great carrier battle at Midway, a turning point of the war in the Pacific Theater. This building is much more than just new administrative offices—it will serve as the Marine Corps' premier cyber warfighting platform, and will provide full spectrum cyberspace operation capabilities. We are on schedule to complete our move in to the Lasswell Building by 4th quarter of fiscal

year 2018, and we anticipate a dedication and ribbon-cutting ceremony to be held sometime this spring.

CONCLUSION

Thank you again, Mr. Chairman and Members of the Committee, for inviting me to testify before you today, and for the support that you and this Committee have provided our marines and their families.

I am incredibly proud of the strides we have made in operationalizing cyberspace in support of the MAGTF and joint warfighter since I was last before you in May, but we have not succeeded alone. Our successes have come from a growing network of partnerships across the Service, the Operating Forces, government, industry, and academia. Cyberspace is a team effort and we are quickly gaining momentum and buy-in to build a more capable, ready force that is prepared to fight—and win-tonight in the cyberspace domain.

I look forward to continuing this dialogue and working with members of this subcommittee in the future.

Senator ROUNDS. Thank you, Major General Reynolds.

Major General Weggeman, you are last because you are the youngest of the branches.

[Laughter.]

Senator ROUNDS. You may begin.

STATEMENT OF MAJOR GENERAL CHRISTOPHER P. WEGGEMAN, USAF, COMMANDER, TWENTY–FOURTH AIR FORCE, AND COMMANDER, AIR FORCES CYBER

Major General WEGGEMAN. I think that's an honor.

Thank you, Chairman Rounds, Ranking Member Nelson, distinguished members of the subcommittee. Thank you for the opportunity to appear before you today along with my esteemed cyber colleagues. I look forward to discussing the Air Force's significant progress in advancing full-spectrum cyberspace operations and our contributions to joint operations.

I have the distinct honor to lead more than 15,000 total-force airmen and civilians 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.

In this domain, threats are growing rapidly and evolving. Our adversaries are acting with precision and boldness, utilizing cyberspace to continuously challenge 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, cybersecurity, and threat-specific defensive operations in order to compete, deter, and win.

The Air Force has invested in the creation, fielding, and sustainment of an ever increasing portfolio of cyber defensive and offensive capabilities. Specifically, seven cyber weapon systems designed to provide a tiered global defense of the Air Force information network; second, defensive cyber maneuver forces to actively defend key cyber terrain; and, last, offensive capabilities to provide all-domain integrated operational effects to combatant commanders.

The Air Force's Cyber Mission Force Teams are on track to achieve full operational capability by the end of fiscal year 2018. As of today, 35 of 39 Cyber Mission Force Teams have declared full operational capability. By comparison, highlighting our extensive progress, at this time, at this same hearing 10 months ago, we only

had nine teams at FOC [Full Operational Capability]. Our four remaining teams are expected to declare FOC by June of 2018, concluding our build phase 3 months ahead of deadline.

Air Force Cyber trains and fights as a total-force team, harnessing the unique attributes and talents of all components—regular Air Force, Air National Guard, and Air Force Reserve. Across 24th Air Force, we employ more than 11,000 full-time and part-time Reserve and Guard personnel providing support for training, intelligence, full-spectrum operations, command and control, and capability development. For our Cyber Mission Force Teams, the Air Force has employed a built-in total-force strategy with 15 Air National Guard squadrons and a classic Reserve associates squadron providing additional trained and ready surge capacity in times of crisis.

Cyberspace operations are powered through partnerships, and 24th Air Force 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. Congressional support continues to be essential to our significant operational progress, and will only increase in importance as we move forward.

I will keep my opening remarks brief, as I have provided a comprehensive update for the committee in my written statement outlining in detail our significant operational improvements, specific initiatives, successes, and challenges, of course.

I am honored and humbled to command this magnanimous organization, and I am inspired every day by the innovative spirit, the patriotism, the sacrifice, and audacity of our Air Force cyber warriors. They are, by far, our Nation's most powerful cyber weapon system.

I look forward to your questions and the ensuing dialogue.

Thank you.

[The prepared statement of General Weggeman follows:]

PREPARED STATEMENT BY MAJOR GENERAL CHRIS P. WEGGEMAN

INTRODUCTION

Chairman Rounds, Ranking Member Nelson, and distinguished members of the Subcommittee, thank you for the opportunity to appear before you today, along with Assistant Secretary of Defense Kenneth Rapuano and 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 orga-

nize, train, and equip functions. Twentyfourth 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 fiscal year 2018. 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 (email, 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 to 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 mis-

sion 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 fiscal year 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-byname 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 percent 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 percent of the Air Force's available E&I and Combat Communications personnel. Twentyfourth 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 $400 million 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 fiscal year 2017, the Air Force garnered $42.7 million 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

The 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 percent. 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 fiscal year 2019, 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 percent (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 $14.2 million, 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 fiscal year 2019.

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.

Senator ROUNDS. Thank you, Major General Weggeman.

Senator Sasse has been a regular attendee at these, and yet he always seems to have to leave before he can ask any questions, and so, I'm going to defer my questions.

Senator Sasse, you may begin.

Senator SASSE. Being 101st in seniority has some downsides, it turns out.

[Laughter.]

Senator SASSE. Thank you, Chairman.

Thank you all for your service. Thanks for being here.

I'd like to talk about the Presidential Policy Directive 20. Does it work? If not, what's the conversation like between you all and DOD and the NSC [National Security Council] about that? Could you talk us through, a little bit, about how long it takes in the process, from beginning to end? All of you, but, General Nakasone, if you want to start.

Lieutenant General NAKASONE. So, PPD–20, or Presidential Policy Directive 20, the methodology upon which we get approval for offensive cyberspace operations, is a work in progress, in terms of the way that we've approached getting approvals. I would say we have had a tremendous amount of success with ongoing operations with regards to JTF [Joint Task Force] Ares and our fight against ISIS. That has been, certainly, something that has allowed us to make a case for the things that we need to have done. Is the proc-

ess perfect? No, it's not. But, this is a constant dialogue that goes on between ourselves, certainly Cyber Command, and the Department of Defense, and then the National Security Council, Senator.

Senator SASSE. Admiral.

Vice Admiral GILDAY.Sir, thanks for the opportunity to comment on this subject.

So, as General Nakasone mentioned, really we have not—PPD–20 hasn't kept us from delivering effects when we have been required to deliver them. It is intended, or was intended, to be a very deliberate process in determining when and how we would deliver cyber effects against—whether it's a sovereign nation or whether it's a rogue actor. I think that—as an overarching policy, I think that it's a good framework. There are built-in mechanisms within that framework to accelerate authorities if we need them. If the Nation needs to get authorities quicker, it exists.

But, as General Nakasone said, we have learned a lot in the last two and a half years. The world has changed a lot in the last two and a half years, in terms of how people act in this space. I do think that we're learning from that, and I do think it's informing policymakers. I think people are marching together to make improvements.

Senator SASSE. So, you can cite specific examples of times when the process has worked, but I assume, if we were in a classified space, there would also be specific operations that you'd tell us about that you were never able to carry out because of how slow it is. I've heard other cyber warriors refer to PPD–20 as molasses. Is it the case? What can we talk about, in a nonclassified setting, about specific operations—I guess not talking about specific operations, but what general takeaways do we have about times when it's been too slow to enable you to act in cases when you had targets that you would have liked to have pursued?

Major General REYNOLDS. Well, I can't speak to any of the operational specifics, but I'll give you a perspective, to your original question. Again, you know, policy is not my realm, as the senior military operational commander, but I'll give you some observations of PPD–20.

Now, when I first came into the domain in 2012, that's when we were writing PPD–20. So, think about the maturation and the pace of change since then. So, 6 years later, we still have the same PPD–20. It started out as kind of an authorities-driven policy directive. I think what we're going to now is, we're learning now that we have capability, capacity to actually do more, we need more of a mission- and risk-informed policy that allows us a broader spectrum of authorities and risks that would allow us the pace, the timing and tempo of operations, I think, to match our adversaries in cyberspace. So, I think that's where we're going now, that we're showing that we have capability, capacity, we're proving ourselves that we can be responsible and credible actors in this space. I think we should be looking at: How do we broader—how do we create a broader spectrum of threat- and risk-based authorities and delegation so that we can respond with greater tempo.

Senator SASSE. I want to follow up on the standardized delegation question, but generally I think you were trying to get——

Major General REYNOLDS. Senator, I would—I mean, I think what you've heard from the other Commanders is exactly that, in that everything that we are learning—I think, every day, we are learning more and more about the delivery of effects in this domain. To General Weggeman's point, it's really a matter of: Where's the risk, and who should accept that risk and—from a decisionmaking perspective? I certainly think there's some room to have more discussion on this, on this PPD, sir.

Senator SASSE. If you were, sort of, briefing the

Armed Services Committee on what standardized delegations might look like for all of our allies, could you give examples of cases where our allies might have some delegated authorities that have been routinized that you'd like us to look at?

Lieutenant General NAKASONE. Certainly, Senator. I'd—I would welcome—probably do that in a different session.

Senator SASSE. I think there are a number of us who'd like to follow up on that and be tutored by you. Again, with all respect to your operational responsibilities, not your policymaking responsibilities, but those of us who are in a policymaking role know well that we need the tutorials of people who are actually living this, day in and day out. So, I'm over time, here, but we'll follow up on that, and invite you back in a classified space.

Thanks.

Senator ROUNDS. Senator Nelson.

Senator NELSON. Mr. Chairman, we're here in the family, so you go ahead.

Senator ROUNDS. All right, thank you. I appreciate it.

I'm going to follow up kind of along the same lines that Senator Sasse has begun. I think it's a good line to begin with.

I'd kind of like to know what limitations and current policy most immediately challenge your ability to operate effectively in cyberspace, if I could. I'll just open this up. We're all in the family here. I recognize that we're in an open session, but we're talking about policy and the difference—and let me perhaps preface this a little bit.

We've got thousands of years of knowing how armies have learned how to interact with one another on a battlefield. There are norms that have been established. The same with the law of the sea. There are norms that have been established, in terms of how we treat one another, military to military, military to civilian, and so forth. Even in the air, we have norms about how one aircraft treats another aircraft when there are incidents. Space is perhaps a little bit newer. Most certainly, the norms there have not been completely established.

When it comes to cyber, the norms are still being established. Our expectation, in many cases, is based upon what norms in other domains of war have already been established. It would seem that our adversaries have not taken the same approach and are not bound by the same respect for norms as perhaps we are.

So, let me bring this back. Again, what are the limitations, in terms of how we look at and how we view the norms, when it comes to our offensive capabilities? What are the limitations that we respect that perhaps you would see in—Senator Sasse has indicated our allies perhaps have other alternatives or other policies

established. We have peer competitors that most certainly do some things that we would not consider to be appropriate at this point, or we are restricted from doing. Do you have any examples of that or things that you have seen that have been frustrating to you with regard to their offensive movements that we simply do not do?

Lieutenant General NAKASONE. So, Senator, normally we're a very talkative bunch. I would offer that we can provide the perspective of our operational lessons learned. Let me take it from that aspect, because I think that's an important piece.

So, when we look at the domain, there are really three things that I think all of us are very interested to have a discussion on. First of all is the discussion of risk. Who accepts the risk? What is the risk? How you describe the risk? What are the mitigations for that risk? They're elements that I think that we talk a lot about when we're—when we are in discussions and planning for cyberspace operations.

Second thing is: What's the operational gain/loss? If we do this mission, or we don't do this mission, what is the opportunity cost for those actions?

The third element, I would say, is: What's the intel gain/loss? That is obviously a question that is offered by many of us and also those in the interagency. I think that that is perhaps the area that all of us, based upon our operational experiences, have spent some time with.

Major General REYNOLDS. Yes, Senator. I guess I—I think I need to offer a thought, based upon Senator Nelson quoting my written statement, because I think this gets right to it.

So, you know, to me, the cornerstone document is our new National Defense Strategy, right? So, compete, deter, and win. So, if I was looking at, you know, a broad set of policies, you know, I don't want to act like the irresponsible actors. I think our—we're a nation of laws. I think we, as military operational commanders, operate under the Law of Armed Conflict, rules of engagement, and special instructions so that we're credible and responsible in the disposition of our duties. But, I do think, if we want to compete, deter, and win in cyberspace, that we have to get, to General Nakasone's point, more oriented on mission outcomes and risk models and threat-driven operations that allow us to become the challenger instead of the challenged in this domain.

So, all the things you mentioned, all the things I talk about, I do think we have to look at new approaches within the confines of our Government and what we seek to do from a national perspective on things like sovereignty. To your point, right? There is no international airspace or water in cyberspace. Every piece of the domain is some manmade space that someone says is his or hers. We have to rethink that. I think we have to look at—becoming the challenger is going to require us to be more of a 21st-century information operation; information warfare-cogent organization or group of interagency partners that wants to then, you know, do the things that are happening to us—to impose costs, to deny benefit, to demonstrate stake, and to convey the legitimacy of those actions to our citizenry, as well.

Senator ROUNDS. Thank you.

Senator Nelson.

Senator NELSON. General Nakasone, you're going to be the Commander of U.S. Cyber Command, and it is now being upgraded to a combatant command. Have you thought about the possible unique role that you're going to be, that you may be one of the U.S. military establishment commanders that is actually in actual combat?

Lieutenant General NAKASONE. Senator, if confirmed, certainly I will be thinking every single day about that, and I have been a bit over the past couple of weeks, as I've testified. I would offer, as I think to this future, it's informed by much of what I've learned over the past couple of years in command of Joint Task Force Ares. If I might——

Senator NELSON. Okay. Let me stop you there. Let me ask about that. Because, as the commander of Task Force Ares responsible for the operations to disrupt ISIS, and specifically to disrupt ISIS on the Internet for their propaganda, recruiting, and command and control, the Task Force's performance in its first year was rated as poor. But, you have testified, "Performance has gotten a lot better." So, have you conducted operations in Task Force Ares designed to manipulate the thinking of ISIS [Islamic State of Iraq and Syria] adherence?

Lieutenant General NAKASONE. Senator, yes, we have. We have conducted information operations. I would offer that that's perhaps the piece of Ares that I've learned the most about, being able to provide a message, to amplify a message to impact our adversaries.

Senator NELSON. So, not just disrupting their networks, but also conducting cognitive information operations?

Lieutenant General NAKASONE. Yes, Senator. In fairness, as you pointed in your opening comment, probably more at the tactical and perhaps operational level. But, I think that that's where it begins, understanding how you provide that message, the infrastructure that you need, the capabilities that are going to underpin your messaging.

Senator NELSON. So, are you using the Army's first Information Operations Brigade?

Lieutenant General NAKASONE. Senator, yes, we are. Certainly that's one of the elements. Other elements for our joint force, to include our marines, our Navy and our Air Force, as well, Senator.

Senator NELSON. So, now you're moving to the strategic level overall, not just the Army's perspective. Are there lessons from this task forward—the task force that can be elevated to the strategic level and applied to the information warfare threat from Russia?

Lieutenant General NAKASONE. Senator, I think there probably are, in terms of the lessons that we've learned in Ares. While I'm a bit hesitant to apply a broad brush, let me offer three that do come to mind.

First of all, you have to start early. You indicated the first year was a difficult one for us. It was a difficult one for us, because we were trying to build an infrastructure, build capabilities, build talent.

The second thing I would offer is: there's nothing more powerful than having your own infrastructure, your own capabilities. One of the things that the Army has provided us is an infrastructure that we use.

The third thing is: it comes down to talent. Eighteen months ago, in a room of, you know, cyberspace operators across our entire force, if I would have asked the question, "Raise your hand if you've conducted an offensive cyberspace operation," out of 100 soldiers, sailors, airmen, and marines, maybe two or three would have done it. Today, nearly the entire room has got their hand up, Senator.

Senator NELSON. So, as you go on to be the four-star commander of a combatant command, Russia has at least some military units that combine technical cyberoperations and information capabilities. The DNI has testified that their operations are having strategic effects on us. That's from Dan Coats, the DNI [Director of National Intelligence]. Do your information operations units have cyber skills?

Lieutenant General NAKASONE. Our information operations units do have cyber skills, Senator.

Senator NELSON. So, if all these functions are integrated at the service level, why do we separate them at the unified command level and in the Office of Secretary of Defense?

Lieutenant General NAKASONE. Well, Senator, I take your point. I think that's where section 1637 of NDAA [National Defense Authorization Act] Fiscal Year 2018 is looking at: How do you bring that together? How do you have one look? I believe that OSD [Office of the Secretary of Defense] is working that piece of it right now, Senator.

Senator NELSON. Okay. As you work that, then you've got to have an answer to the question: Who is responsible for strategic information operations, the kind of operation that Russia has conducted against us in our elections? Anything you can comment on that in this setting at this time, even though you don't have the fourth star?

Lieutenant General NAKASONE. So, Senator, I will wait until the OSD has completed that study there. I think that that's important as we take look and move forward over.

Senator NELSON. Okay.

I'll just close out, Mr. Chairman, by saying that it was so telling when Admiral Rogers, our four-star commander, whom General Nakasone will relieve when Admiral Rogers retires—it was so telling that he said he's ready to do the attacks, but he has not been given the authorities. I fear for American democratic institutions if we don't attack.

Thank you, Mr. Chairman.

Senator ROUNDS. Senator McCaskill.

Senator MCCASKILL. Thank you.

Well, I would just like to speak briefly to you about a couple of issues. One is recruitment and retention of the personnel that we need in terms of the cyber fight. You know, there are many things about the Defense Officer Personnel Management Act that I think enhances the strength of our military, but there's also some things about it that don't seem to make much sense in certain contexts. I really would love to get your all's input as to how the up-or-out issue relates to the expertise we need in cyber. You know, I know that pilots in the Army can typically be warrant officers who can progress in rank but still continue to fly. Have we made the adjust-

ments for cyber warriors to be able to adjust in rank and still be able to work in the cyber sector? Or are we defaulting to the norm, which is moving them out of that MSO [Military Service Obligation] into something different so that they can get experience throughout the various parts of our excellent military?

So, I'd like each of you to address briefly the recruitment-and-retention issues and what issues that DOPMA [Defense Office Personnel Management Act] may be causing for our retention of the very best in this really challenging field? We have enough trouble competing with the private sector without adding in some of the challenges that are inherent in the current way that we develop leadership in our military.

Admiral?

Vice Admiral GILDAY.Senator, good afternoon. Thanks for your question.

So, if I could say real briefly, in terms of constraints, I think we have direct commission programs now, where we're trying to attract the best and the brightest from society to join us. So, their entry level is at an ensign or a second lieutenant. That pay is about $37,000 a year base pay. So, we are not competitive with the private sector, in terms of competing for that kind of talent. We want to go after it. Similarly——

Senator MCCASKILL. I get—I mean, you know, we can't—I mean, that's what we pay somebody to answer the phones in—around here. We're asking them to have incredible expertise. That seems to me totally unrealistic.

Vice Admiral GILDAY.Yes, ma'am. There have been other hearings on the Hill recently where this has been addressed by the personnel chiefs, in terms of requesting additional relief so that we can give people credit for their years of service in the outside sector and pay them what they deserve, in terms of being competitive with the private sector.

In terms of up-or-out, we have not made any modifications yet, although we know we're going to have to take a look at that and do so in the future. Because, to your point, we're just going to hemorrhage talent at that—at those upper ranks, when we really don't need to. We could retain those people longer.

If I could talk about the civilian force for a moment, that's where we do have some challenges, in terms of some fairly rigid guidelines that we have to follow, in terms of the amount of incentives that we can offer people coming in. Maybe a 10-percent hiring raise, maybe a 10-percent relocation bonus; perhaps, in some cases, accelerated promotion—but, not broadly enough to make us a very attractive employer for those in the private sector.

I think that the Cyber Excepted Service is a step in the right direction, in terms of providing us more latitude. But, I still think the—I still think that we will likely need more authorities to remain competitive, or to be competitive, with the private sector.

Senator MCCASKILL. Is there any other input that anyone would like to give on this subject?

Major General REYNOLDS. Senator, I would just say that I agree with everything that Admiral Gilday said. I think cyber is going to be the game-changer for us. We, in the Marine Corps, just established the new MOS so that we could target incentives. Already, I

think, we're going to maximize the bonus structure that we have inside the Marine Corps to kind of get after and retain some of this special talent. The Commandant makes the point all the time, you know, "We may end up with a platoon of warrant officers, and that's got to be okay with us." So, I know, at the highest level of our service, he's willing to challenge status quo. The key for us is to figure out what exactly is that incentive? In some cases, ma'am, it's not pay. Sometimes it's education, sometimes it's certificates, sometimes it's—you know, so, for us, it's being able to target those incentives and have the freedom of action to do that to retain the best talent, ma'am.

Senator MCCASKILL. Anybody else?

Lieutenant General NAKASONE. I would add to General Reynolds' point. For the Army, what we have taken a look at is our career fields. So, Senator, as you discussed the challenge with DOPMA right now, you know, up or out, what we have looked at is: Is there a career field out there for a tool developer that all he's going to do for 20 years is develop these exquisite tools? We think there is. One of the things that I have seen, across all the Services, the senior leadership to, you know, try new flexibility on these things. Are we going to send enlisted soldiers to get a graduate degree? Are we going to send them to training with industry? Are we going to do different type of activities that will be attractive to them? Not all of them will work. Some of them will. But, unless we try some of these things, I think that, you know, we're going to have a challenge in the future.

Senator MCCASKILL. Well, if you have the flexibility with MOS descriptions and MOS incentives, then that's one thing, but I would really appreciate—if there are things that we could add to the NDAA this year to give you more tools to recruit and retain—there is no question that, if there is one area that I pretty much believe, on a bipartisan basis, everyone realizes that we have got to up our game, it is in cyber warfare, because clearly, right now, I would not say that we're winning. I don't like it when we're not winning. Some of that is complicated by policy decisions, but some of it is us getting the very best and the very brightest.

If there are specific things we could do to give you additional flexibility or tools, I'd really appreciate it if you would share them with us before we begin our consideration of the NDAA this year.

Senator ROUNDS. I recognize that you are over on time, but I know that General Weggeman had tried to make a comment, as well, and I would allow General Weggeman to respond, as well, if he'd like to at this time.

Major General REYNOLDS. Yeah, I think my compatriots provided most of the responses. For me, I personally believe the Services recruit, first, based upon values, and then, second, based upon talent or skillset. I think the cornerstone we have as cyberspace operations professionals is our mission. As you all know, we're the only organization that has the mission to do what we do, when directed and authorized, legally. I look at that as the biggest retention tool we have. Is like—it's like young Captain Weggeman on the F–16 line. When I flew four times a week, I was as happy as they get. Give me any mission, send me anywhere. I'm up for it. It's the same for our cyber operations professionals. You know, reps and

sets. So, we have to make sure we're giving them the tools, the infrastructures, and the environments so that they can sharpen and hone their tradecraft, so they get those sorties. That helps with retention, for sure.

But, you know, the second thing that would help us all is, we're all working together. I think we're working with industry on cutting-edge assessment tools to assess a cyber aptitude of an individual when they come in front of us. What—you know, the interesting I—thing I learned from the people—again, I'm not a technologist, ma'am, I'm a fighter pilot by training, but what I've learned is, the biggest thing we ask them, to assess them, is: What do you do in your home time? Are you scripting on Python? Are you on a Metasploit? Are you coding? Are you taking Raspberry Pis and putting them together? Are you—that's actually one of the best, most powerful assessment tools, so that's one of the things that we ask them, in terms of that.

I think you've given us a lot of the powerful arrows in our quiver, which is to direct assess and direct commission. The Air Force has—our—in 15 days from now, our first two pilot direct commissionees go to OTS [Officer Training School]. One will be a second lieutenant, one will be a first lieutenant. So, we appreciate that.

We'll certainly get back to you on what we could ask of you in the next NDAA. But, I just wanted to offer the mission perspective as being the cornerstone for retention, from my perspective.

Senator MCCASKILL. Thank you.

Thank you, Mr. Chairman.

Senator ROUNDS. Thank you.

Senator Gillibrand.

Senator GILLIBRAND. Thank you, Mr. Chairman.

I just want to say, I agree with Senator McCaskill, strongly, that, please give us a request for authorities on any of the issues where you need support, resources, flexibility, whatever it is, any ideas.

[The information referred to follows:]

ARCYBER could use additional assistance from Congress in recruiting and retaining technically skilled talent from the civilian sector. While we appreciate being given statutory authority to offer constructive credit to potential cyber officers, that authority is currently limited with respect to offering military rank commensurate with civilian sector abilities, experience and education. The Department of Defense submitted a legislative proposal for inclusion in the Fiscal Year 2019 National Defense Authorization Act (NDAA), which expands constructive credit up to the rank of colonel, in both the Active and Reserve components. This would afford us greater discretion in determining the rank of the appointed officer, providing the Army a more robust means by which to recruit and retain soldiers with skills critical to the Army's cyber mission. As of the date of submission of this IFR Insert, LTG Stephen G. Fogarty is the commander of ARCYBER.

Senator GILLIBRAND. I talked to Lieutenant General about this before. So, anything you need, we will provide, because we feel so passionately about this.

For Generals Nakasone and Weggeman, you're both building out Reserve components for cyber capability right now. The Guard has now built a new—out—Task Force Echo, which has been deployed to Fort Meade. General Nakasone, what do you see as the long-term mission of the Army Guard cyber component?

Lieutenant General NAKASONE. Senator, you referenced our Guard component, we'll build 11 teams over the next 4 years. They

will be doing both State missions, when not activated, and they will also be doing such things as Task Force Echo, which is a mobilized mission to protect our infrastructure.

What we have found, working with the Guard, are several elements. First of all, incredible base of talent. Secondly is the ability to provide them the same training standard that our Active component gets. The third thing is to equip them with the same tools that we use on the Active side and the Reserve side. That's powerful for us, ma'am.

Senator GILLIBRAND. I think you agree with this, but could the Guard help address some of the existing gaps in our whole-of-nation approach to cyber? Could it serve as a conduit between State, local, and Federal Government, as well as the private sector, because of the unique relationships on the ground and authorities?

Lieutenant General NAKASONE. I do agree, Senator.

Senator GILLIBRAND. General Weggeman?

Major General REYNOLDS. Thank you, ma'am. Yes, I'll go first—last question first.

So, absolutely. I think the Air National Guard of the 262 Cyber Operations Squadron in Washington State is a great exemplar of how you can partner with State utilities, and now they're working through the legal dimension of even a private-sector utility, for how we would provide support from a—an industrial base SCADA [Supervisory Control and Data Acquisition] system support and electrical power SCADA system support. So, that's the Guard, the citizen airmen in that State, helping both their State and private-sector utilities. That's actually ongoing. They have three dedicated ten-person UTCs—think of them as deployable teams—that are specialized in EP, electrical power, SCADA systems, as one example to this. So, we're already—I think that they're a great exemplar to go to.

In terms of, you know, the Air Force, we've built in, in our CMF [Cyber Mission Force] build, Guard and Reserve capabilities already. So, right now we have 15 Guard cyber squadrons that have contributed to build three of the Active Duty CMF teams—two cyber protection teams and one national mission team. They're currently—actually, the Guard forces from New York, New Jersey, and Texas are the three——

Senator GILLIBRAND. Great.

General REYNOLDS.—States currently manning those teams. They've gone through ten full mobilization rotations. So, in dwell right now, the Air Force already has ten cyber protection teams in the Guard in dwell for surge capacity, if required.

Senator GILLIBRAND. I'd like to ask you, for the record, both of you, for a—recommendations in terms of how we could use the National Guard to support next year's election from cyberattack as a critical infrastructure. I understand, from earlier hearings, that you don't feel you have that authority from the President. But, what I would like from this committee is recommendations to this committee that, if you were given that authority, what you would like to implement and what resources or support you would need to implement that specific mission. I will then use that. Because this is something that both Senator Rounds and Nelson have been very focused on, because we do see the election as critical infra-

structure. We do see an attack on our election infrastructure as a declaration of war. I want to know, if we ever were able to give you the authority to protect the next election, how you would use the National Guard, specifically, to do that, and what additional either resources or authorities you would need if you were tasked with that duty. Because that's something this committee has been very focused on for a long time, and we'd like your input, specifically, if we were to do that in the NDAA.

[The information referred to follows:]

Normally, unless called into Federal service, National Guard support to elections is within the purview, and subject to the direction, of each state governor. Governors can choose to activate National Guard personnel in a State Active Duty status at any time they deem necessary and appropriate. U.S. Army Cyber Command executes its Title 10 training and readiness oversight of Army National Guard (ARNG) cyber forces by managing personnel in approved cyber training courses and ensuring that cyber protection teams (CPTs) meet USCYBERCOM established joint standards directed for all Army components. Any additional specialty training concerning election systems would be at the discretion of the relevant state governor. The Army is resourced to build a total of 11 ARNG CPTs, one of which will reach initial operational capability in September 2018, with all reaching full operational capability by 2022. Once at full operational capacity, the ARNG teams will have the training and equipment to support a range of missions defending critical infrastructure. Currently, our cyber forces execute both the Federal and state level missions. As we fully establish these forces, our ability to support directed operations will only improve. As of the date of submission of this IFR Insert, LTG Stephen G. Fogarty is the commander of ARCYBER.

Major General REYNOLDS. Okay. So, I appreciate, ma'am, giving the latitude that—if the policy was given and the authorities were given, I think there's two specific things that I think are essential, and it kind of goes to the fire forces we've learned that can fight fires, and it goes to pre-scripted knowledge and missions. Unless you want us to be what I would call a "wet cleanup on aisle five force," if you want us to be there and preventatively build security——

Senator GILLIBRAND. Correct.

General REYNOLDS.—and defense to thwart malicious cyberactivities, we would need the authorities and the tools and the infrastructure—some of our defensive kits—that are purposely tailored to the networks and systems that you would want us to support the State and local SCADA—or, sorry, infrastructure CICR systems with. So, you know, we need to know the networked topology, we need to know the hardware, firmware, software that it operates so that we could be responsive, we could sensor, we could share information, and we could be proactive in defense.

Senator GILLIBRAND. So, that is the guidance I'd like you to write to this committee by letter to say, "If we were ever given this responsibility, if we were ever given this authority, these are the ten things we would need." That's item number one. "We would need access to all the information and systems that are used, State by State. We would need access to the resources to be able to develop expertise in each of these systems. We would need X, Y, and Z."

So, just tactically, what do you need? Then, we can at least, as a committee, decide: Do we want to put that in the NDAA as authorities for you to then go ahead and do? Obviously, the President would have to sign off on that. But, as our work from the committee, we've had so many hearings on cyber, specifically, and I feel like your hands have been tied every time we talk about one crit-

ical infrastructure, which is our electoral system. We already know we have foreign adversaries who are hammering it daily. We also know that you—that we now have the technology, because we had a hack-a-thon and actually effectively hacked vote totals. Our own cyber experts could do that within, I think, a 24-hour period. So, we know what the vulnerabilities are. I just want to proactively know from you guys, with your expertise, what you would need if I was—if you were told you need to prevent this and you need to start a new mission.

Major General REYNOLDS. Yes, ma'am.

Senator GILLIBRAND. So, just guidance, so we know what it looks like. We also have several private-sector think tanks working on this, as well, what would be their recommendations to go to every one of the 50 Secretaries of State. We'll have that information soon enough. We have a bill with—Senator Graham and I—to create a 9/11-style deep dive to assess what are the vulnerabilities and what are the ten things, as a secondary effort, too. But, in the meantime, I'd like your guidance, because if we can put it in the NDAA in April—or, when is the—it's soon. It'll be soon.

Senator ROUNDS. We're in the middle of it now.

Senator GILLIBRAND. Yeah, right now. So, it'll be soon when we get to vote on it.

Thank you.

Senator ROUNDS. Senator Nelson, I know that you're time-constrained, but if you'd like to make some comments or questions here, we'll do that before we start to finish up here a little bit.

Senator NELSON. Thanks.

General Nakasone, on the issue of direct commissioning, what are the legal limits that you cite? Should we alter them so that this program can be successful?

Lieutenant General NAKASONE. Senator, what we are facing right now is an inability to grant constructive credit. As Admiral Gilday spoke to, constructive credit is the recognition of someone's abilities or experience in the civilian sector transformed and measured against what rank they may come in within the military. Right now, I believe that we are limited to first lieutenant—bringing them in as a first lieutenant. So, we would like greater flexibility on that, based upon greater experience.

I think that's important when you think about some of the capabilities and some of the talent we're looking for—people in big data, artificial intelligence, machine learning, forensics malware analysis. Those are all things that are not necessarily attractive to come in as a young first lieutenant.

Senator NELSON. Do you think that's hampering us getting people to join?

Lieutenant General NAKASONE. I do, Senator.

Senator NELSON. So, how do you fix that? Put them at a higher rank?

Lieutenant General NAKASONE. So, one of the things we've been working with your staffers is to look at how we better measure constructive credit to allow them to come in at a higher grade.

Senator NELSON. General Reynolds, tell me, if a—if you get a direct commission into the Marine Corps, does that mean that they still have to be able to do 15 pull-ups?

Major General REYNOLDS. Yes, sir.

Senator NELSON. Good.

[Laughter.]

Senator NELSON. I'm glad, General.

Why should cyberspace be any different from other domains? Do we need the legislation to establish, without a doubt, that traditional military activities include cyber operations?

Well, General Nakasone, you're going to be the big chief——

[Laughter.]

Senator NELSON.—so why don't you try to answer that?

Lieutenant General NAKASONE. So, I don't think it should be any different than the other domains, Senator. I think that this has been a product of, you know, a very, very young and maturing force that we have, you know, some unique capabilities and characteristics of how we operate. Not having borders is something that, you know, really isn't applicable in the other domains, minus space. So, one of the things that we, again, have come to is, you know, being able to define traditional military activities has sometimes been hard. It's much harder if you're not operating in this space. Now that we are continually operating in this space, I think we have a much greater way of being able to determine what traditional military activities are.

Senator NELSON. Thank you.

Senator ROUNDS. Admiral Gilday.

Senator NELSON. Sure.

Vice Admiral GILDAY.Briefly. Sir, I'm—I respect your time, as you want to depart. The comment that I'd make with respect to cyber and traditional military activities is that the longer that it takes to integrate cyber into the other warfighting domains, the longer it takes to normalize it, the less—the longer it takes for people to get comfortable with it, and the more it's treated as a special kind of action that it's difficult to get authorities for.

To the point that you made in your opening comments about the Russians—and it's related to this—we're at a point right now where we've allowed the Russians to establish those boundaries. We have allowed them—in any other space—the maritime, the air, the land—you want to gain access so that you can dominate. You want to put the enemy—you want to be in a position to dominate, whether it's physically or, in this case, virtually. The Russians, the Chinese, the North Koreans, when you talk about authorities, they have different rule sets, they have a lower threshold for aggression. So, they are gaining the initiative. So, it becomes more difficult for us to gain a position of advantage and to do the things that you want us to do.

Changing policy is one thing. The will to act is a completely different problem set that is just as important as changing PPD–20 or changing any policies that underlie how we act in this space.

Senator ROUNDS. Thank you.

I'm going to follow up on this, because I think this really gets to the root of a lot of the questions that you've heard today, and comments that you've heard today. I know that Senator Gillibrand has discussed the issue of the electoral process and how critical that is. But, I think you can look at almost any of our critical infrastructure right now and you can just simply ask the same question, and

that is, If this was act of war or if this was an act of aggression using kinetic forces, whether by air, land, or sea, there would be an expectation by the American public that our defense forces would be in a position to respond, to defend? But, then also there would be an expectation that the deterrent forces would come to bear. Seems that with regard to cyber, we have yet to establish what those incidents are and at what point they reach the point to where there has to be a deterrent reaction on our part.

The Defense Science Board made it very clear that with—for the next 10 years, our defensive capabilities will not be equal to the offensive capabilities of our peer competitors. It's become very clear—and I think the discussion—and, Admiral Gilday, I think you made mention to it—Russia has a different norm, in terms of what they see as the opportunities within the cyber domain. I think we've seen that with a number of the peer competitors and also some rogues, as well. That is, is that they have used cyber as a way to impact our Nation's—our assets—in some cases, critical infrastructure and, in some cases, an electoral process. But, most certainly, they do it right now without a sense that we're prepared to offer that deterrence.

Can we talk a little bit about what it would take and about the challenges—not so much—and I recognize that this is an open session, but I think it's really important to lay out, you know, as I said, that—when we talk about NATO issues and so forth, and we talk about international norms, there is Tallinn 1 and there is Tallinn 2.0, both of which try to establish what rises to an act of war in cyberspace and also what the incidents are that have to be responded to. Isn't it really true that, here, we have huge defensive capabilities, and that we have huge capabilities with regard to being able to infiltrate silently and gather a huge amount of data, as good as anybody in the world, and yet, at the same time, because we want to make sure that we follow the norms and that we are a respected neighbor, that we are very, very careful about how we respond in the domain of cyber? If it was air, land, or sea, there could be hell to pay, but in cyber we're not quite prepared to identify and to state publicly what those norms are.

What are the policy discussions—and if I had a group of enlisted men and women sitting in front of me right now who are on the front lines doing this, and it was in a classified setting, they would spill their guts about how frustrated they can be at times and what they would really love to be able to do, but they recognize their responsibility to adhere to clear policy choices.

I know this is more of a statement than it is a question, but it's your turn now. You've thought about this a lot. Can you, in this open space, talk a little bit about the challenges that you see, and perhaps some of the frustrations that you have, in terms of protecting our critical infrastructure, civilian resources, and so forth, that perhaps the public simply doesn't recognize and that we should be talking about more?

Lieutenant General NAKASONE. Senator, I'll begin on this. This is a very important question.

So, I think it begins with: What is the strategy for the defense of the Nation in cyberspace? That is an overall question that I

think has to be asked, has to be debated, has to be discussed amongst policymakers, the American people, and others.

Senator ROUNDS. Would you—let me just stop you right there. Fair to say that we really don't have a true cyber policy established yet?

Lieutenant General NAKASONE. So, I've learned, from my testimony over the past couple of weeks, Senator, that this committee has asked many times for a policy, and that one still has not been delivered. That's correct.

Senator ROUNDS. Okay.

Lieutenant General NAKASONE. I would offer that, when we think about other defense of the Nation in cyberspace—roles, responsibilities, functions, missions—what are the elements that make it up? What are the parts of the government, what's the responsibility of the private sector that owns 90 percent of the networks that are necessary to protect?

The next thing I think about a lot is: What are the thresholds of support? So, when we think about this, how much of this responsibility should reside with the private sector, and at what point, when a nation-state actor has taken after our critical infrastructure, does it become the responsibility of the Department of Defense to defend the Nation? That is still a discussion point that I think is, you know, one to be had.

So, those are just a couple, Senator, that I would offer as I've thought about this question over the past several months.

Senator ROUNDS. General Reynolds.

Major General REYNOLDS. Yes, sir. I'd like to just add one or two thoughts on this.

One of them is that—I guess in my time in command at MARFORCYBER, going back to the Defense Science Board and what they learned about, you know, deterrence, one of the key findings was that we need to be able to deny the adversary. I don't want to speak for all of my peers here, sir, but we have spent an enormous amount of time even inside the service on this denial piece: How we make sure that what I own is defensible? There was a lot of work to do. So, moving forward, will we have additional capacity? Yes, sir, I think we would.

But, the other thing that I would like to make sure that we make a point here, in that—and it goes back to the JTF Ares lessons learned. What Ares did, I think, for U.S. Cyber Command was provide a—number one, a joint capability inside U.S. Cyber Command, so you have all the Services represented there, but it also gave an opportunity for the combatant commands to reach into Cyber Command. In one single entry point, it gave the interagency one place, it gave our allies and partners one place to come in the counter-ISIL [Islamic State of Iraq and the Levant] fight. That was enormously important.

So, I think, organizationally, moving forward: Who are the other combatant commanders that are involved in the plan against Russia? How are we organizing ourselves? It's really essential, Senator.

Senator ROUNDS. Thank you.

General Gilday.

Vice Admiral GILDAY.Sure. Thanks for your question.

The main point that I want to make is that the force is not big enough, not based on the discussion that we had in this room this afternoon. If there's expectations to protect critical infrastructure, to hold significant adversaries at risk, adversaries that we are in contact with every day, then more needs to be done, in terms of the buildout and the development of a cyberforce that is comparable to the Nation's reliance on cyberspace for our economy, for our quality of life. It touches everything that we do. It's gigantic. And you take a look at the force, and you take a look at the number of trigger-pullers we have, 6,200—6,200. Take a look at the United States Navy, take a look at the United States Army, take a look at the Marine Corps, the smallest of the Services, and the Air Force, and make a comparison there. Based on what we talked about this afternoon in this room, the importance of cyberspace to the American people, to our quality of life, I think that that has to, at some point, be reassessed. I think that the things that we have learned over the last 2 years need to play into that assessment. I think we need to be honest with ourselves. I think we need to act more boldly.

Senator ROUNDS. General Weggeman.

Major General REYNOLDS. There's a benefit of going last. I think a lot of the key points I would make—to Admiral Gilday's last point, I agree. The scope and scale of CICR is extremely vast. And I agree, our force is too small. So, we will have to think deliberately and calculated, in terms of what would be DOD's role in—to support that, and how do we best use a high-demand, low-density force, if a policy is written to where we would provide that, above and beyond the National Guard or the Reserves?

You know, so, as the former J5 at Cyber Command, I've been thinking about, you know, the cyber deterrence question for a long time, and I'll give you, simplistically, my frame.

The first thing is, the phrase is flawed. I believe the proper way to say it is "cyber indeterrence." Cyber—it's—what is cyberspace operations' role, offense and defense, in a national strategic deterrence campaign? Admiral Rogers testified that, you know, sometimes you don't want to use cyber when you come back. So, it's got to be a whole-of-government, if not whole-of-nation, campaign.

The second thing about any indeterrence is: Deter what? I think what we constantly come back to in this forum is, we want to say we want to deter malicious cyber activity. So, if we want to deter or erode an enemy's confidence in their ability to pitch malicious cyber activity at us, again, we need to use every arrow in our quiver as a nation to deter that activity. We are but one. We may be the least—have the least amount of capability or capacity. So, we have to go to other things. But, I do think it's all about "cyber indeterrence," and that's really important.

I go back to the classic principles of, you know, within cyber we have to be able to impose cost, we have to be able to deny benefit, and maybe we do one in the cyberspace domain and other in another domain, whether it's land, sea, maritime, information, leveraging State Department or FBI [Federal Bureau of Investigation] or other agency partners.

The last is the concept of—in the Defense Science Board study, everything is about taking that first hit. It's a constant thing. For

those of us who have been around, this is an offense-dominant domain. Our adversaries have exquisite capabilities. If you want to be that second-strike force, you may not have that luxury. It's hard to recover. So, I think we have to do a hard look at a nation, given the exquisite insights that our intelligence community can generate, the exquisite insights that our cyber forces and operators can generate. What is the—what is our realm of strategic preemption? When would we have thresholds or triggers where we would strategically preempt a large release of malware that would take us down and set us back on our feet for a year?

Senator ROUNDS. Thank you.

Now, let me just finish with this. General Nakasone, the Ares project, they pointed out earlier that there were some challenges there, and that some of the conditions weren't the best. And yet, unless we clearly look at and we—we're critical in the way that we analyze our successes and where we need to improve, we're not really doing our job. So, the fact that we could have a frank discussion about improvements and so forth, that's a positive thing. Showing how far we've come in a very short period of time with regard to this particular domain, I think, is critical in creating more successful opportunities in the future. If we ever get to the point where we can't look at those criticisms and say, "These are learning experiences, and we can do better, and we will learn from them," then we're in real trouble.

So, I—first of all, I don't take offense from someone suggesting that there were challenges with a program and that we're going to have to do better in the future. I think that's the way that it was perceived by the panel that's before us today. I appreciate that.

Second of all, I think what we've talked about here today, while we're talking about the positioning, the capabilities of our forces today from your perspective, I think what you've given us, in terms of an insight as far as what the policy issues are and the understanding of the American public with regard to your mission right now and the role that you have been asked to play, versus what I think in many cases is the expectation of an American public that says, to begin with, "If someone attacks us in cyberspace, we should hit them hard in cyberspace" versus—the appropriate role is—just because someone attacks us by sea doesn't mean we necessarily have to attack only by sea. We can attack in a whole lot of different domains. But, it does require this, that unless we are dominant in air, land, sea, space, and cyber, our adversaries will take advantage of any opening they see.

And so, with that, I want to say thank you to Senator Gillibrand for being able to attend with us again today. I want to thank all of our witnesses here today for your testimony. This is not the last that we will see you all in front of our committee again.

And, General Nakasone, we look forward to visiting with you in a new role, as well, when the opportunity comes.

And unless any one of our witnesses has anything further to add, we will call an adjournment to this meeting at this time.

Thank you.

[Whereupon, at 3:49 p.m., the subcommittee adjourned.]

○