NOT FOR PUBLICATION UNTIL RELEASED BY
THE SENATE ARMED SERVICES COMMITTEE
CYBERSECURITY SUBCOMMITTEE

STATEMENT BY

VICE ADMIRAL MICHAEL M. GILDAY

COMMANDER

U.S. FLEET CYBER COMMAND

U.S. TENTH FLEET

BEFORE THE

SENATE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON CYBERSECURITY

CYBER POSTURE

1ST SESSION 115TH CONGRESS

MAY 23, 2017

NOT FOR PUBLICATION UNTIL RELEASED BY
THE SENATE ARMED SERVICES COMMITTEE
CYBERSECURITY SUBCOMMITTEE

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, the U.S. Tenth Fleet, and the United States Navy. It is a privilege to represent those outstanding Sailors and civilians who comprise our Fleet Cyber/Tenth Fleet team, and I appreciate this opportunity to update you on how our Navy's cyberspace operations are evolving to remain competitive in a changing strategic environment.

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), Information Operations, Electronic Warfare, Cyber, 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, Md., U.S. Fleet Cyber Command exercises operational control of globally-deployed forces 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 command and control of full spectrum cyberspace operations for assigned Cyber Mission Force teams.

U.S. Fleet Cyber Command's operational force comprises nearly 16,500 Active Duty and Reserve Component Sailors and civilians organized into 24 active commands and 32 reserve commands around the globe. The commands are operationally organized into a Tenth Fleet-subordinate task force structure for execution of operational mission. More than 35 percent of U.S. Fleet Cyber Command's operational forces are directly aligned to execute our cyberspace operations missions.

In the two years since my predecessor VADM Jan Tighe last testified before the Emerging Threats Subcommittee in April 2015, we developed and released our *Strategic Plan 2015-2020.* This plan charts our course to deliver on our responsibilities by leveraging our strengths and shrinking the Navy's vulnerabilities to a cyber adversary, which I detail throughout this statement. Across the wide-ranging responsibilities, we identified 5 strategic goals:

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 Cyber Mission Teams and plan for the sustainability of these teams over time.

Since that time, we, as a command, along with our fellow Service Components, U.S. Cyber Command, and the Department of Defense (DoD), have continued developing organizationally, as well as evolving cyberspace capabilities and capacity. I thank you for opportunity to discuss the Navy's progress in cyberspace, where we have made much progress and are moving out smartly on the course ahead.

Operate the Network as a Warfighting Platform

We operate in an increasingly competitive 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 not only degrades our confidence and effectiveness of our C2, it also leads to loss of intellectual property and dulls our competitive edge. The margins of victory are razor thin, and we cannot afford to lose a step. To help ensure we retain our competitive edge, the forces of Fleet Cyber Command and the Tenth Fleet are highly integrated with our Navy's regional Fleet Commanders they support and are fully integrated to current and future Fleet operations so we may flex and adjust our cyberspace capabilities to maximize success of any assigned mission. Our leadership is fully supportive of U.S. Fleet Forces Command and U.S. Pacific Fleet's focus on distributed maritime operations and Fleet-centric warfighting.

U.S. Fleet Cyber Command directs operations to secure, operate, and defend Navy networks within the Department of Defense Information Networks (DoDIN). I can most succinctly capture our approach to cybersecurity by stating the Navy operates is networks as a warfighting platform. This concept has many facets, including as a warfighting platform it must be aggressively defended from intrusion, exploitation and attack. As a warfighting platform, the network must be agile and resilient and responsive to the C2, intelligence, logistics, and combat support functions that depend upon it. As a warfighting platform, it must be capable of and available to deliver warfighting effects in support of Combatant Commander operational priorities.

The Navy Networking Environment currently consists of more than 500,000 end user devices; an estimated 75,000 network devices (e.g., servers, domain controllers); and approximately 45,000 applications and systems across three security enclaves. Reflective of the larger culture, the demand for interconnectedness continues to grow and cybersecurity solutions must keep pace.

Today's Navy's Enterprise Networks have benefited greatly from the nearly 1 billion dollar executed and proposed investments (through FY 20) that reduce the risk of successful cyberspace operations against the Navy Networking Environment.

The Navy took such aggressive actions implementing lessons learned during Operation Rolling Tide, during which U.S. Fleet Cyber Command fought through an adversary intrusion into the Navy's unclassified network. Some of our best investments have not only been in technology, but in the development of policies and Tactics, Techniques and Procedures. This investment of time and focus enabled significantly increased visibility into and more importantly increased awareness of the state of Navy's Enterprise Networks.

It was through the lens of our post-Operation Rolling Tide efforts that the Navy identified where immediate infusion of defensive network capabilities was most critical and where accelerated modernization of network infrastructure was most warranted.

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 behaviors, and supply chain anomalies. 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 are not rapidly deployed across our networks, systems, and applications. The attack surface also grows larger when network users, unaware of the ramifications of their on-line behavior exercise poor cyber hygiene and unwittingly succumb to spear phishing emails that link and download malicious software, or use peer-to-peer file sharing software that introduces malware to our networks, or simply plug their personal electronic device into a computer to recharge it.

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, and improving the process on how we inspect the cyber readiness of our networks. Furthermore, we are bolstering our ability to manage cyber security risks in our networks through our certification and accreditation process, and through working with industry partners and academia on ways to utilize data analytics, machine learning, and other automation technologies. 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 contract. Incorporating lessons-learned from Operation Rolling Tide, a large-scale network maneuver and operation to eradicate and adversary from the Navy's unclassified network, and combining our overseas networks into the Navy Marines Corps Intranet (NMCI), will offer improved situational awareness, ability to C2, operate and defend the network. Extending our CONUS NMCI to our OCONUS Network (ONE-Net) will leverage the operational and security capabilities of the NMCI and the unique requirements of our overseas warfighters, reducing the network attack surfaces. The improved situational awareness capability in NGEN-R will provide our headquarters and network defense subordinate forces the ability to make better informed network operational decisions, improving our network response actions, reducing the network intrusion attack surface and decreasing response time.

Often times, people are viewed as the largest vulnerability in this equation – by that same logic, we believe our people, each and every person touching a keyboard, can make the network stronger. In addition to cyber awareness training for all hands, we are working closely with U.S. Cyber Command to develop an innovative and robust persistent training environment for our network defenders. We are also working closely with the U.S. Naval Academy, the Naval Postgraduate School, and the U.S. Naval War College on ways to increase the relevance and currency of their cybersecurity and cyberspace operations education programs and initiatives.

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 through layered sensors and countermeasures from the interface with the public internet down to the individual computers that make up the Navy Networking Environment. We configure these defenses by leveraging 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 mutual defense.

We cannot and will not assure our mission in this domain alone. We operate in and around an infrastructure that is largely commercially owned. The rise of dual-use technology has created vulnerabilities, but should just as well be leveraged for opportunity. Many of our challenges are not unique to the .mil domain. We fend off the same spectrum of adversaries, who are using the same playbooks against .govs and .coms. We work to plug and patch the same legacy networks. Industry is and will remain a critical mission partner through both technology development and responsible information sharing.

We are also piloting and deploying new sensor capabilities to improve our ability to detect adversary activity as early as possible. This includes increasing the diversity of sensors on our networks, moving beyond strictly signature-based capabilities to behavioral sensing, and improving our ability to detect new and unknown malware. We also have the need to be able to analyze this sensor data at "machine speed," and are working with partners to investigate ways to utilize emerging data sciences technologies to help with the analysis of our networks.

I firmly believe the future lies in automation and machine learning for defense. Not only does this change the dynamic of speed and scale, but it allows us to use our people where they are most needed.

As my predecessor noted in her 2015 testimony, 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. 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 and industrial control systems. Additionally, the Navy is transitioning 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. 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. This 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.

Together, these actions will help us to truly build cybersecurity and resilience in at the beginning of system development and avoid the pitfalls associated with trying to bolt it on at the end.

The Joint Information Environment's Joint Regional Security Stacks 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 Joint Regional Security Stacks (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 Joint Information Environment's Joint Regional Security Stacks will allow shared visibility into the boundary capabilities for Navy and DOD integrated DODIN.

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. To succeed, we must understand both side's vulnerabilities and the potential consequences within both systems. To that end, we work to mature our abilities to detect, analyze, report, and take action in and through our Networks. The Navy has started 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). Additionally, we are working with our SPAWAR and NAVSEA acquisition partners to improve the network sensor information we can collect across our platforms into a single dedicated big data analytics platform that will bring with it a new level of fidelity and agility to our warfighting. This data strategy will enable us to work seamlessly with all DoD network operations and maritime operations data. The SHARKCAGE platform will allow for better overall situational awareness and improved speed of response to the most dangerous malicious activity by leveraging the power of machine learning and artificial intelligence to harness existing knowledge more rapidly. Building cyber situational awareness from the maritime tactical edge back, will bring with it a superior Joint warfighting force that will be capable of maneuvering through the electromagnetic spectrum and fight resiliently in the age of informationalized warfare.

U.S. Fleet Cyber Command Operational Forces

Status of the Cyber Mission Force

The Cyber Mission Force is designed to accomplish three primary missions: National Mission Teams will defend the nation against national level threats, Combat Mission Teams to support combatant commander priorities and missions, and Cyber Protection Teams to defend Department of Defense information networks and improve network security.

Navy and other cyber service components are building these teams for U.S. Cyber Command by manning, training, and certifying them to the U.S. Cyber Command standards. Navy teams are organized into 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 as well as their supporting teams consisting of three National Support Teams and five Combat Support Teams.

The Navy is currently on track to have full operational capability for all 40 Navy-sourced Cyber Mission Force Teams in 2018. As of 1 April 2017, we had 26 teams at final operating capability. We are in the process of manning, training, and equipping our teams to be FOC ahead to the October 2018 deadline. Additionally, by October 1st of this year, 298 cyber reserve billets will augment the Cyber Force manning plan.

Over the past year, 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 this was an area where organizationally we have recently made progress. As a JFHQ-C Commander, I required an extension of my staff at PACOM to integrate cyberspace planning and force employment into Geographic Combatant Command operations alongside forces from other domains. So in February of this year, I organized my Cyber Mission Force teams in Hawaii to form an interim Cyber Forward Element as a one-stop-shop for full spectrum cyberspace operations in support of PACOM until permanent manning is available to support the Geographic Combatant Command. This Fleet Cyber Command-Forward Element is not a new command, but rather an extension of my staff to provide Offensive and Defensive Cyberspace planning to PACOM on a permanent basis. Our planning with PACOM must be robust enough to create cyber support plans that are integrated into their operational plans. This required a staff that is fully embedded into the supported daily battle rhythm processes while relying upon reach back to, and support from, my main staff at the Headquarters. This forward element has already improved relationship with PACOM in the short time they have been established, and it allows me to have the functionality and capacity I require to effectively C2 my operational Cyber Forces, which include three USAF CMF teams and two US Army CMF teams, as well as my Navy Cyber Mission Forces.

Reserve Cyber Mission Forces

Through ongoing mission analysis of the Navy Total Force Integration Strategy, we developed a Reserve Cyber Mission Force Integration Strategy that leverages our Reserve Sailors' military and civilian skills and expertise to maximize the Reserve Component's support to the full spectrum of cyber mission areas. Based on this mission analysis, we like other services see the maximum value from our Reserve element within the high-priority Defensive Cyber Operations area. Accordingly the 298 Reserve billets, of which the final phase will come into service in October, are being individually aligned to Active Duty Cyber Protection Teams and the Joint Force Headquarters-Cyber. Each of these Navy-sourced teams will maximize its assigned Reserve Sailors' particular expertise and skill sets to augment each team's mission capabilities, rather than as a one-for-one replacement of team workroles. In this way, we can ensure access to the unique skillsets our Reserve Sailors bring to the fight, while at the same time building a cadre of highly trained personnel that can be called on 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 Cyber Mission Force Integration Strategy and adapt as necessary to develop and maintain an indispensably viable and sustainable Navy Reserve Force contribution to the Cyber Mission Force.

Recruit and Retain

In FY2016, the Navy met officer and enlisted cyber accession goals, and is on track to meet accession goals in FY2017. 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 within each of these ratings are eligible for Selective Reenlistment Bonus (SRB). SRB 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, we have requested, and anticipate approval of Special Duty Assignment Pay (SDAP) for one of most critical skills sets, Interactive On-Net Operators (IONs). SDAP would provide a monthly stipend of $200-$500.

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.

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 workroles throughout the CMF and 44 are our Computer Scientists/Tool Developers. Currently we have 27 of the 47 positions filled throughout CMF; are in the initial recruitment phase for our 44 Tool Developers and have made 13 other selections to date. We are aggressively hiring to our civilian authorizations consistent with our operational needs and fully supported by the Navy's priority to ensure health of the cyber workforce. We have also initiated a pilot internship program with a local university to recruit skilled civilian and military cyber workforce professionals. Navy will measure the success of this approach as a potential model to harness the nation's emerging cyber talent. Our primary challenges in recruiting are the current compensation allowable and competition with industry and other DoD entities. With this in in mind, we are now offering various incentives to potential candidates which includes higher step (step 7) on the GS pay scale, 10% of salary as a one-time recruitment incentive, 10% 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 NSA.

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

Educate, Train, Maintain

To develop officers to succeed in the increasingly complex cyberspace environment, the U.S. Naval Academy offers introductory cyber courses for all freshman and juniors to baseline knowledge. Additionally, USNA began a Cyber Operations major in the fall of 2013, and in 2016, 27 Midshipmen were the first to graduate with the degree. This year, 46 Midshipmen will graduate with the degree and 72 have entered the major. Furthermore, the Center for Cyber Security Studies harmonizes cyber efforts across the Naval Academy.

Our Naval Reserve Officer Training Corps' (NROTC) program maintains affiliations at 51 of the 180 National Security Agency (NSA) Centers of Academic Excellence (CAE) at colleges around the country. Qualified and selected graduates can commission as Cryptologic Warfare Officers, Information Professional Officers, or Intelligence Officers within the Information Warfare Community.

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 Operations and Technology, and Applied Mathematics, Operations Analysis, and Defense Analysis. Naval War College is incorporating cyber into its strategic and operational level war courses, at both intermediate and senior graduate-course levels. The College also integrates strategic cyber research into focused Information Operations (IO)/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, including a whole-of-government Cyber war game under active consideration for this coming summer or fall.

With respect to training of the Cyber Mission Force, U.S. Cyber Command mandates Joint Cyberspace Training & Certification Standards, which encompass procedures, guidelines, and qualifications for individual and collective training. U.S. Cyber Command with the Service Cyber Components has identified the advanced training required to fulfill specialized work-roles in the Cyber Mission Force. Most of the training today is delivered by U.S. Cyber Command and the National Security Agency in a federated but integrated approach that utilizes existing schoolhouses and sharing of resources. The Navy is unified in efforts with the other Services to build Joint Cyber training capability, leveraging Joint training opportunities, and driving towards a common standard. 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.

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 as we build out the balance of Cyber Mission Force.

We will depend upon commands across the Navy to recruit, train, educate, retain and maintain this workforce including the Chief of Naval Personnel, Navy Recruiting Command, Naval Education and Training Command and Navy's Institutions of Higher Education (United States Naval Academy, Naval Postgraduate School, and Naval War College.) Additionally, the establishment of Naval Information Forces (NAVIFOR) in 2014 as a Type Commander has made a significant impact in generating readiness for cyber mission requirements. NAVIFOR works closely with the Man, Train, and Equip organizations across the Navy to ensure that U.S. Fleet Cyber Command and other Information Warfare operational commands achieve proper readiness to meet mission requirements. Navy is now enhancing the NAVIFOR capability with the establishment of the Naval Information Warfare Development Command (NIWDC), newly established in 2017, to advance the maturing of Information Warfare, including cyberspace operations, doctrine, training, Tactics, Techniques & Procedures (TT&P).

Fleet Readiness

The Navy's 2018 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 Cyber Mission Forces, 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 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 the investments are 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 common operational picture (COP) at our Fleet Maritime Operations Centers.

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

Your Navy has recognized that we have not only witnessed a changing and evolving cast of competitors, but the very nature of our strategic environment has changed. We are witnessing a return to great power competition. In the Chief of Naval Operations' Campaign Design for Maritime Superiority, he points to the rise of the global information system and the rate of technological creation and adoption as two of the dominant global forces shaping the maritime environment our Navy must operate, and if called upon, fight in. Cyberspace will be a contested environment and we cannot take freedom of maneuver for granted. It is clear that our reliance on our networks will not diminish as we push toward distributed maritime operations.

U.S. Navy freedom of action in cyberspace is necessary for all missions that our nation expects us to be capable of carrying out including winning wars, deterring aggression and maintaining freedom of the seas.

There is no individual success, at least not in the long term. We will succeed by leveraging our strengths and shrinking our vulnerabilities. Operational success will be built upon a strong network of partners (DoD, Interagency, Industry and Academia), a resilient, defensible infrastructure, and complemented by our greatest resource and asymmetric advantage – our people.

Thank you again for this opportunity to update you on great work being done by the men and women of Fleet Cyber Command, 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 these cyber investments included in the Navy's 2018 budget request. I'm happy to take your questions.