NOT FOR PUBLICATION UNTIL RELEASED
BY THE SENATE ARMED SERVICES
COMMITTEE SUBCOMMITTEE ON
EMERGING THREATS AND CAPABILITIES

STATEMENT

OF

VICE ADMIRAL JAN E. TIGHE
COMMANDER, U.S. FLEET CYBER COMMAND/U.S. TENTH FLEET

BEFORE THE

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

OF THE

SENATE ARMED SERVICES COMMITTEE

ON

CYBER OPERATIONS

April 14, 2015

NOT FOR PUBLICATION UNTIL RELEASED BY THE
SENATE ARMED SERVICES COMMITTEE
SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

Chairwoman Fischer, Ranking Member Nelson and distinguished members of the Subcommittee, thank you for your support to our military and the opportunity to appear before you today along with my military service component counterparts and partners.

Madame Chairwoman, I have been in command of U.S. Fleet Cyber Command and U.S. TENTH Fleet for just over one year. U.S. Fleet Cyber Command reports directly to the Chief of Naval Operations as an Echelon II command and is responsible for Navy Networks, Cryptology, Signals Intelligence, Information Operations, Electronic Warfare, Cyber, and Space. As such, U.S. Fleet Cyber Command serves as the Navy Component Command to U.S. Strategic Command and U.S. Cyber Command, and the Navy's Service Cryptologic Component Commander under the National Security Agency/Central Security Service, exercising operational control of U.S. Fleet Cyber Command operational forces through TENTH Fleet. Specifically, we conduct cyberspace operations to ensure Navy and Joint or Combined forces' freedom of action while denying the same to our adversaries.

The commissioning of U.S. Fleet Cyber Command and reestablishment of U.S. TENTH Fleet on January 29, 2010 closely followed the Navy's 2009 acknowledgement of information's centrality to maritime warfighting, known as Information Dominance. Information Dominance is defined as the operational advantage gained from fully integrating the Navy's information functions, capabilities, and resources to optimize decision making and maximize warfighting effects. The three pillars of Information Dominance are assured command and control (C2), battlespace awareness, and integrated fires. U.S. Fleet Cyber Command is a key warfighting element in delivering on missions across those three pillars.

Since my U.S. Fleet Cyber Command predecessor ADM Michael S. Rogers last testified before this Subcommittee in July 2012, the Department of Defense (DoD), U.S. Cyber Command, and the Service Components have significantly matured cyber operations and enhanced cyber operational capabilities. I appreciate the opportunity to outline the Navy's progress over the past two years, where we are headed to address an ever increasing threat, and how budgetary uncertainty is likely to impact our operations.

Cyber Operations, Posture, and Future Investments

U.S. Fleet Cyber Command directs operations to secure, operate, and defend Navy networks within the Department of Defense Information Networks (DoDIN). We operate the Navy Networking Environment as a warfighting platform, which must be aggressively defended from intrusion, exploitation and attack. The Navy Networking Environment consists of more than 500,000 end user devices; an estimated 75,000 network devices (servers, domain controllers); and approximately 45,000 applications and systems across three security enclaves.

Operations during the past two years led to a fundamental shift in how we operate and defend in cyberspace. Specifically, late summer 2013 we fought through an adversary intrusion into the Navy's unclassified network. Under a named operation, known as OPERATION ROLLING TIDE, U.S. Fleet Cyber Command drove out the intruder through exceptional collaboration with affected Navy leaders, U.S. Cyber Command, National Security Agency, Defense Information Systems Agency (DISA), and our fellow service cyber components. Although any intrusion upon our networks is troubling, this operation also served as a learning opportunity that has both matured the way we operate and defend our networks in cyberspace, and simultaneously highlighted gaps in both our cybersecurity posture and defensive operational capabilities. As a result of this operation and other cybersecurity initiatives, the Navy has already made or proposed (through FY20) a nearly 1 billion dollar investment that reduce the risk of successful cyberspace operations against the Navy Networking Environment. Of course these investments are built on the premise that our future year budgets will not be drastically reduced by sequestration. Specifically, if budget uncertainty continues, we will have an increasingly difficult time fully addressing this very real and present danger to our national security and maritime warfighting capability.

The Navy's future cybersecurity investments are being informed by the Navy's Task Force Cyber Awakening, which was chartered by the Chief of Naval Operations and the Assistant Secretary of the Navy for Research, Development and Acquisition to gain a holistic view of cybersecurity risk across the Navy, and beyond just our corporate navy networks to include

combat and industrial control systems. The FY16 Proposed Budget (PB16) includes Task Force Cyber Awakening -recommended investments amounting to $248M for FY16 and $721M across the Future Years Defense Plan (FYDP). Task Force Cyber Awakening will make additional recommendations on how to organize and resource capabilities to mitigate that risk.

Concomitant with the Task Force Cyber Awakening outcomes is the migration to a single defensible Cyber architecture, which is vital to the continued success of Navy's worldwide operations. The Navy recognizes that the Joint Information Environment (JIE) is an operational imperative and endorses that vision, including the implementation of a single security architecture (SSA). The Department of the Navy intends for the Navy and Marine Corps Intranet (NMCI) to serve as the primary onramps into JIE, incorporating JIE technical standards through our network technical refreshment processes as those standards are defined. Through delivery of these enterprise environments, the Navy will achieve the tenets of JIE's framework of standards and architecture consistency.

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 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 behaviors, and supply chain anomalies with counterfeit devices from untrusted sources. Operationally, we think of these opportunities in terms of the network intrusion attack surface presented to malicious cyber actors. The greater the attack surface, the greater the risk to the Navy mission. The attack surface grows larger 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. Furthermore, we are bolstering our ability to manage cyber security risks in our networks through our certification and accreditation process, and through cyber security inspections across the Navy. Additionally, the Navy is reducing the attack surface with significant investments and consolidation of our ashore and afloat networks with modernization upgrades to the Next Generation Enterprise Network (NGEN) and the Consolidated Afloat Networks and Enterprise Services (CANES), respectively. Finally, the Navy is executing a Data Consolidation Center (DCC) strategy, which will reduce the number and variance of information systems at the same time allow for a centralized approach towards managing the confidentiality, integrity and availability of our data.

For long term success in cyber security, the Navy is working on improved acquisition and system sustainment processes. Specifically, we will design in resiliency by generating a common set of standards and protocols for programs to use as guiding principles during procurement, implementation, and the configuration of solutions, which will improve our cyber posture by driving down variance.

The Navy recognizes that all hands (users, operators, program managers, systems commands…) have an impact (for better or worse) on the magnitude of the Navy's attack surface and the mission risk associated with it. U.S. Fleet Cyber Command must defend this attack surface, regardless of size, using defense in depth capabilities described below.

Defense in Depth

The Navy is working closely with U.S. Cyber Command, NSA/CSS, our Cyber Service Partners, DISA, Interagency 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.

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 include reputation-based and heuristic capabilities), and improving our ability to detect new and unknown malware.

JIE Joint Regional Security Stacks are also integral to our future defense in depth capabilities. As described above, the Navy has already consolidated our networks behind defensive sensors and countermeasures. We expect that JIE Joint Regional Security Stacks (JRSS) v2.0 will be the first increment to bring equal or greater capability to Navy Defense in Depth. 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.

Cyber Situational Awareness

Success in cyberspace requires vigilance: it requires that we constantly monitor and analyze Navy Networking Environment. We must understand both its availability and vulnerabilities. Furthermore we must be able to detect, analyze, report, and mitigate any suspicious or malicious activity in our Networks. The Navy is planning to expand our current capabilities to include a more robust, globally populated and mission-tailorable cyber common operating picture (COP). Additionally, with improved network sensor information across the DoD, however, comes the need for a single dedicated data strategy and big data analytics for all DoD network operations and defense data. This will allow for better overall situational awareness and improved speed of response to the most dangerous malicious activity by leveraging the power of big data analytics to harness existing knowledge rapidly.

U.S. Fleet Cyber Command Operational Forces

U.S. Fleet Cyber Command's operational force comprises nearly 15,000 Active and Reserve sailors and civilians organized into 22 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. Approximately 35 percent of U.S. Fleet Cyber Command 's operational forces are aligned with the cyber mission.

Status of the Cyber Mission Force

As you may recall, during a hearing before the Senate Committee on Armed Services on March 12, 2013, General Keith Alexander briefed the Cyber Mission Force model, which DoD endorsed in December 2012. 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 personnel assigned for all 40 Navy-sourced Cyber Mission Force Teams in 2016 with full operational capability in the following year. As of 1 March 2015, we had 22 teams at initial operating capability (IOC) and 2 teams at full operational capability (FOC). We are in the process of manning, training, and equipping our FY15 teams to meet IOC standards by the end of FY15. Additionally, between now and 2018, 298 cyber reserve billets will also augment the Cyber Force manning plan as described below.

U.S. Fleet Cyber Command has also been designated as the Joint Force Headquarters-Cyber by U.S. Cyber Command to support U.S. Pacific Command and U.S. Southern Command in the development, oversight, planning and command and control of full spectrum cyberspace operations that are executed through attached Combat Mission and Support Teams. In 2014,

Navy's Joint Force Headquarters-Cyber was certified and declared to have achieved Full Operational Capability. This capability was attained without additional U.S. Fleet Cyber Command resources. As the Cyber Mission and Support Teams continue to grow and mature, additional resources to operationally control and manage these teams in support of Combatant Command Priorities will be required.

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' skill sets and expertise to maximize the Reserve Component's support to the full spectrum of cyber mission areas. Within this strategy, the 298 Reserve billets, which are phasing into service from FY15 through FY18, will be individually aligned to Active Duty Cyber Mission Force teams and the Joint Force Headquarters-Cyber. Accordingly, the Joint Force Headquarters-Cyber and each Navy-sourced team will maximize its assigned Reserve Sailors' particular expertise and skill sets to augment each team's mission capabilities. As our Reserve Cyber Mission billets come online and are manned 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.

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 and as we refine our needs to holistically address the challenges being informed by Task Force Cyber Awakening. 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 Navy Information Dominance Force (NAVIDFOR) in 2014 as a Type Commander will go a long way in generating readiness for cyber mission requirements. NAVIDFOR will work closely with the Man, Train, and Equip organizations

across the Navy to ensure that U.S. Fleet Cyber Command and other Information Dominance operational commands achieve proper readiness to meet mission requirements.

Recruit and Retain

There are many young Americans with the skill sets we need who want to serve their country. I am very encouraged by the dedication and commitment I see entering our ranks. I am awed by their dedication and growing expertise every day. We must consistently recruit and retain this technically proficient group of diverse professionals for the cyber mission to sustain this momentum.

In FY2014, the Navy met officer and enlisted cyber accession goals, and is on track to meet accession goals in FY2015. 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.

Cyber-related officer communities are also meeting retention goals. While both Information Warfare (IW) and Information Professional (IP) communities experienced growth associated with increased cyber missions, we are retaining officers in these communities at 93 percent overall. Both IW 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 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.

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. 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 Information Warfare Officers, Information Professional Officers, or Intelligence Officers within the Information Dominance Corps.

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, 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.

Declining Budgets

While the overall Navy budget has been impacted by financial constraints and sequestration, the Navy has done a good job in terms of minimizing the budgetary impact on U.S. Fleet Cyber Command and the capabilities it employs to conduct its operations. Should this circumstance change and future budgets decline, however, there will be an impact to the capability and capacity to conduct operations in cyberspace. The scope and magnitude of such impacts would be driven by the scope and magnitude of a budget decline.

It is, however, possible to speak in broad terms regarding the potential areas of impact. Operations in cyberspace are highly dependent on people - to a certain extent our people are part of the warfighting platform in cyberspace. Budgetary declines impacting our ability to attract and retain the numbers of people with the requisite skills and experience would negatively impact the Navy's ability to conduct operations in cyberspace. Additionally, declining budgets affecting the ability of the Navy to implement initiatives described above that reduce the network intrusion attack surface, enhance defense in depth and cyber situational awareness, or modernize/migrate to the Joint Information Environment greatly jeopardizes the Navy’s ability to accomplish all missions, since all Navy mission accomplishment depends on having an available and secure network. Finally, reductions to procurement accounts, beyond cyber operations- or network-specific budgets, traditionally have delayed or slowed modernization of programs across the Navy. The unintended consequence of delayed modernization is delayed cyber vulnerability remediation in everything from business applications to weapon systems.

Summary

Our success in the maritime domain and joint operational environment depends on our ability to maintain freedom of maneuver and deliver effects within cyberspace. To ensure operational success in the maritime and other warfighting domains, defense of Navy and DoD networks and information is essential and cannot be separated from the overall maritime operational level of war.

In order to continue to progress in cyberspace operations, we must have sufficient resources to ensure we close any identified cybersecurity gaps and provide our workforce with the right capabilities to maintain our warfighting advantage. We must be prepared – both technologically and with skilled operators, civilian and uniformed - and remain innovative. The threat in cyberspace will only continue to grow despite our budgetary challenges. 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.

I thank you for this opportunity to share U.S. Navy and U.S. Fleet Cyber Command operations and initiatives in cyberspace.