POSTURE STATEMENT OF

VICE ADMIRAL ROSS MYERS

COMMANDER, UNITED STATES FLEET CYBER COMMAND

BEFORE THE 117TH CONGRESS

SENATE ARMED SERVICES COMMITTEE
SUBCOMMITTEE FOR CYBERSECURITY

APRIL 05, 2022

Chairman Manchin, Ranking Member Rounds, and distinguished Members of the Subcommittee, thank you for the opportunity to testify today, and for your continued interest and support of the United States Navy, including the Sailors and Civilians at U.S. Fleet Cyber Command, U.S. Navy Space Command and U.S. Tenth Fleet.

As you are aware, the cyber challenges facing our nation have grown year over year since Fleet Cyber Command was established just over a decade ago. The cyber domain encompasses the entire globe and extends into space to challenge competitors who operate in the gray zone with the intent of doing our nation harm. Under the leadership of U.S. Cyber Command, the combined efforts of the Cyber Service components represents a unity of effort that underpins the nation's strategic advantage in the cyber domain. That advantage is built upon a professional workforce that leads in innovating and implementing cyber capabilities. To support that effort, U.S. Fleet Cyber Command fully employs more than 14,000 professionals and 40 Cyber Mission Force teams in 16 countries and territories to deliver offensive and defensive cyber effects. With the support of 29 reserve commands, we also have the flexibility to surge forces to meet emerging requirements in our assigned areas of operation in the Pacific and South America, or as tasked. In addition, Navy's cyber forces operate and defend the Navy's expansive, global network - including the sensor grid, communications systems, modem defenses and more than 750,000 user accounts - afloat and ashore. These efforts enable the nation to maintain maritime superiority from the seafloor to space.

Today's reality and that of current events demands that we have an unrelenting operational focus with foresight and ruthless self-assessment to maintain the nation's strategic advantage in cyberspace. I am committed to this approach and have tasked my force to do the same.

In that vein, our forces are delivering capabilities *daily.* Cyber Protection Teams are deployed around the world to operate and maintain critical Navy communications networks. They are prepositioned to respond to crisis, as well as conduct integrated exercises and planning with partners and allies to increase combined cyber capabilities. Cyber Mission Force teams are postured to provide response options to achieve national security objectives.

We have a lot to be proud of, and we continue to grow. Using the Chief of Naval Operations' "Get Real, Get Better" approach, we are taking a hard look at ways to recruit, retain, train and employ our forces to sustain readiness and remain a premier force. We are 'all in' on improving fleet readiness by using data to identify root problems as well as solutions. We owe that to our workforce. We owe that to our Nation.

Fleet Cyber Command shares many of the same concerns as the remainder of the Joint Force regarding challenges caused by competing in a very tight labor market for a small pool of qualified, highly talented applicants. Therefore, Fleet Cyber Command is actively using the array of authorities given by Congress to address today's recruiting, retention and training challenges. For example:

- To recruit, Navy is marketing and advertising in every zip code via traditional means, as well as digital and social media. We are also partnering with Science, Technology Engineering and Math (STEM) institutions.

- To retain, we are offering lucrative promotion opportunities and merit reorder for officers - as well as advancement opportunities, special pay up to $300 per month and reenlistment bonuses up to $90,000 for enlisted personnel.
- To train, we are using requested resources to create three Force Generation elements at current Cyber Mission Force team concentration sites in Maryland, Florida and Hawaii to accelerate the timeline to produce fully trained and qualified personnel.

Conclusion

The cyber warfighting domain is growing at break neck speed and the required investment by competitors to gain entry is low. Thus, maintaining a superior force is a key challenge that requires constant vigilance. Fleet Cyber is primed to adhere to that high standard.

Thank you, again, Chairman Manchin and members of this committee for allowing me to appear before you today to provide an update on the status of Navy's cyber readiness efforts. Your continued support allows us to remain ready to defend networks and conduct cyber operations to support national defense objectives around the globe. While facing unprecedented challenges, I am confident we are building the right workforce to compete and win in this emerging, warfighting domain.