THE SECRETARY OF THE NAVY

March 12, 2019

On October 12, 2018 I asked a group of subject matter experts to review the Department of the Navy's cybersecurity posture. This group teamed with current operational military and civilian experts to compare Navy's cybersecurity governance structures against best practices from both government and industry for alignment of authority, accountability, and responsibility.

The report highlights the value of data and the need to modify our business and data hygiene processes in order to protect data as a resource. This review also provides an assessment of the culture, people, governance, processes, and resources as they pertain to cybersecurity in the Department of the Navy. Recommendations in the review specifically address policy, processes, and resources needed to enhance cyber defense and increase resiliency.

With urgency the Department of the Navy Secretariat along with the Chief of Naval Operations and the Commandant of the Marine Corps, will coordinate with the Department of Defense and Congress for the resources required to compete and win in the cyber domain.

Leadership has already initiated this process as part of a broader review of how best to organize the Department to address the overall challenges of information management; to include not only cybersecurity, but also data strategy and readiness, business system rationalization, and artificial intelligence. We will be working with the Congress to determine what legislative authorities may be required to implement any significant changes.

I thank the review team for their efforts and comprehensive research and analysis. Their exploration of best practices in both industry and government provides the Navy a clear path forward as the Department addresses this challenge.

Richard V. Spencer