



RESEARCH
AND ENGINEERING

THE UNDER SECRETARY OF DEFENSE

3030 DEFENSE PENTAGON
WASHINGTON, DC 20301-3000

21 Jan 2021

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Terms of Reference – Defense Science Board Task Force on Future Cyber Warfighting Capabilities of the Department of Defense

Section 1655 of the National Defense Authorization Act for Fiscal Year (FY) 2020 (Public Law 116-92) requires the Secretary of Defense direct the Defense Science Board (DSB) to conduct a study on future cyber warfighting capabilities. I am tasking the DSB, through the establishment of the Task Force on Future Cyber Warfighting Capabilities of the Department of Defense, to undertake this study.

The Joint Cyber Warfighting Architecture (JCWA) was developed to integrate the collective strengths of Department of Defense cyberspace capabilities to build the 21st century statecraft necessary to understand, contest, and impose high costs on an adversary that is rapidly evolving. JCWA provides the organizing architectural framework for this integration – defining, synchronizing, and deconflicting the holistic set of cyberspace resources to function as a cohesive whole rather than disparate parts. Each of the major functional areas of the JCWA will be tightly integrated and automated to allow United States Cyber Command (USCYBERCOM) to rapidly shift the entire Cyberspace Enterprise in a coordinated and consistent manner to maneuver at the scale and scope of Combatant Command objectives.

Over the past 10 years, our adversaries have defined the space we are operating in, conducting actions that have largely been uncontested – stealing our intellectual property, leveraging stolen Personally Identifiable Information of American citizens, and attempting to interfere in our Democratic processes. Our responses were reactive, focused on shoring up defenses against exploitation while the adversaries had already moved on to far more impactful, disruptive, and destructive actions.

Persistent engagement must be the Nation's foundational approach to taking on near-peer adversaries. We must bring the cyber fight to the adversary by impacting their actions, imposing costs for those activities, and sending a message that we will contest their attempts to disrupt and destroy our national security and democracy. Taking on near-peer adversaries, and ultimately getting ahead of them, requires USCYBERCOM to bring to bear all cyberspace resources at any time in a cooperative engagement. All opportunities afforded by integrated offensive, defensive, and Department of Defense Information Network operations must be leveraged to learn about the adversary, assess risk, and decide on a coordinated response approach. When fully fielded by the end of FY 2024, the JCWA will enable USCYBERCOM to orchestrate planning and execution at the pace of cyber by automatically shifting and turning resources as an interoperable system of systems. This study will focus on the following areas as outlined in Section 1655 of the National Defense Authorization Act for Fiscal Year 2020 (Public Law 116-92):

CLEARED
For Open Publication

4
Feb 18, 2021

- A technical evaluation of the Joint Cyber Warfighting Architecture of the Department, especially the Unified Platform, Joint Cyber Command and Control, and Persistent Cyber Training Environment, including with respect to the following:
 1. The suitability of the requirements and, as relevant, the delivered capability of such architecture to modern cyber warfighting.
 2. Such requirements or capabilities as may be absent or underemphasized in such architecture.
 3. The speed of development and acquisition as compared to mission need.
 4. Identification of potential duplication of efforts among the programs and concepts evaluated.
 5. The coherence of such architecture with the National Mission Teams and Combat Mission Teams of the Cyber Mission Force, as constituted and organized on the day before the date of the enactment of this Act.
 6. The coherence of such architecture with the Cyber Protection Teams of the Cyber Mission Force and the cybersecurity service providers of the Department, as constituted and organized on the day before the date of the enactment of this Act.
 7. The coherence of such architecture with the concepts of persistent engagement and defending forward as incorporated in the 2018 Department of Defense Cyber Strategy, including with respect to operational concepts such as consistent spy-on-spy engagement, securing adversary operating pictures, and preemptively feeding indicators and warning to defensive operators.

- A technical evaluation of the tool development and acquisition programs of the Department, including with respect to the following:
 1. The suitability of planned tool suite and cyber armory constructs of the USCYBERCOM to modern cyber warfighting.
 2. The speed of development and acquisition as compared to mission need.
 3. The resourcing and effectiveness of the internal tool development of the USCYBERCOM as compared to the tool development of the National Security Agency.
 4. The resourcing and effectiveness of the internal tool development of the USCYBERCOM as compared to its acquisition.
 5. The coherence of such programs with the concepts of persistent engagement and defending forward as incorporated in the 2018 Department of Defense Cyber Strategy, including with respect to operational concepts such as consistent spy-on-spy engagement, securing adversary operating pictures, and preemptively feeding indicators and warning to defensive operators.

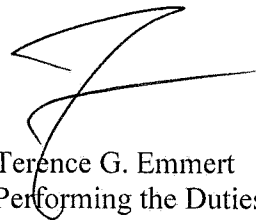
- An evaluation of the operational planning and targeting of the USCYBERCOM, including support for regional combatant commands, and suitability for modern cyber warfighting.

- Development of such recommendations as the Board may have for legislative or administrative action relating to the future cyber warfighting capabilities of the Department.

The DSB Study's findings, observations, and recommendations will be presented to the full DSB for its thorough, open discussion and deliberation at a properly noticed and public meeting subject to Government In Sunshine Act requirements. The Under Secretary of Defense for Research and Engineering (USD(R&E)) will serve as the Department of Defense decision-maker for the matter under consideration and will, as such, take into consideration other stakeholders identified by the study's findings and recommendations. The nominal start date of the study period will be within 30 days of the initial appointment of its members, and Section 1655 of the National Defense Authorization Act requires a report be submitted no later than November 1, 2021. In no event, will the duration of the study exceed 24 months from the start date.

The study members are granted access to those Department of Defense officials and data necessary for the appropriate conduct of their studies. As such, the Office of the Secretary of Defense and Component Heads are requested to cooperate and promptly facilitate requests by DSB staff regarding access to relevant personnel and information deemed necessary, as directed by paragraphs 5.1.8. and 5.3.4. of Department of Defense Instruction 5105.04, "Department of Defense Federal Advisory Committee Management Program," and in conformance with applicable security classifications.

The DSB and the DSB Study will operate in accordance with the provisions of the Federal Advisory Committee Act, the Government in the Sunshine Act, and other applicable federal statutes, regulations, and policy." Individual DSB and DSB Study members do not have the authority to make decisions or recommendations on behalf of the DSB nor report directly to any Federal representative. The members of the task group and the Board are subject to certain Federal ethics laws, including 18 U.S. Code §208, governing conflicts of interest, and the Standards of Ethical Conduct regulations in 5 C.F.R., Part 2635).



Terence G. Emmert
Performing the Duties of the
Under Secretary of Defense
for Research and Engineering