THE UNDER SECRETARY OF DEFENSE
3030 DEFENSE PENTAGON
WASHINGTON, DC 20301-3030

RESEARCH
AND ENGINEERING

OCT 3 0 2019

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Terms of Reference – Defense Science Board Task Force on Department of Defense Dependencies on Critical Infrastructure

The Department of Defense (DoD) lacks a holistic, end-to-end understanding of—and limited ability to mitigate—the impact of degradation and failures in critical infrastructure on which force projection and the functioning of defense critical assets depend. This shortcoming stems in part from the fact that the vast majority of critical infrastructure is owned by the private sector and assigned to other agencies or departments for infrastructure protection coordination and/or regulation. But an equally important factor is that DoD's engagement with key sectors to understand the degree to which the Department is reliant on their services and to educate those owners on what would be most important to the Department for sustaining operations in a time of crisis is both limited and nascent. Compounding the problem, it is unclear who is—or should be—the lead for addressing and ensuring the remediation of critical infrastructure issues within DoD. Back-up plans, where they exist, have not been adequately red teamed and provisioned to ensure the flow of forces, or availability of adequate power or materiel (outside of minimum installation power and supplies) in the face of major infrastructure outages.

Congress has recognized one aspect of the problem. The 2019 Defense Authorization Bill (section 1649) directs the Assistant Secretary of Defense for Homeland Defense Global Security in the Office of the Under Secretary of Defense (Policy) to carry out a pilot program to model cyber attacks on critical infrastructure to identify and develop means for improving DoD's responses to requests for Defense Support for Civil Authorities (DSCA) for such attacks. But the scope of what's needed is much broader than impacts to the DSCA mission. In the event of a major attack on key critical infrastructure sectors—particularly energy (e.g., the electric grid and oil/gas transmission and distribution), water, transportation, communications, and the Defense Industrial Base (DIB)—the ability to project force, to ensure the capability to deploy, distribute, and sustain forces and logistics, and to have confidence in critical command and control elements could be compromised or even eliminated.

The Defense Science Board is asked to form a task force charged to investigate DoD's dependencies on non-DoD owned critical infrastructure with a focus on the energy, water, transportation, and communications sectors, and potential vulnerabilities and consequences from intentional multi-domain attacks against them. The Task Force should also assess how well the Department has addressed any issues related to its reliance on the DIB, for which it has direct responsibility. Key questions that should be considered include:

- What are the most serious threats and vulnerabilities to these sectors?

- What are DoD's assumptions about operating in a contested homeland environment, and do these assumptions adequately address the evolving threat environment?

- What are the potential impacts to DoD operations and/or assets should an attack compromise or eliminate sector capabilities for days to weeks?

- How well prepared is DoD to mitigate the consequences of outages, lack of availability, or compromises to the information flow within the sectors that affect its operations?

- What steps should the Department take to improve its resiliency to the loss or degradation of infrastructure sector services critical to its operations, especially in a crisis environment in which military deployments have been ordered?

- How can DoD partner with other agencies, as well as with private sector partners (directly), to ensure at least a minimum essential level of availability of key infrastructure supporting critical DoD missions in any circumstance?

- How can DoD promote regional resilience/secure enclaves including resilience of critical nodes beyond just its fence line?

The Task Force is encouraged to engage other departments or agencies within the government, as well as infrastructure owners, in order to develop as complete an assessment as possible.

I will sponsor the study. Dr. Miriam John and Hon. Judith Miller will serve as the co-Chairmen of this study. Mr. Jan Ithier will serve as the Executive Secretary. Mr. Kevin Doxey will serve as the Defense Science Board Secretariat.

The task force members are granted access to those DoD officials and data necessary for the appropriate conduct of their study. The Under Secretary of Defense for Research and Engineering will serve as the DoD decision-maker for the matter under consideration and will coordinate decision-making as appropriate with other stakeholders identified by the study's findings and recommendations. The nominal start date of the study period will be within three months of signing this Terms of Reference, and the study period will be between 9-12 months. The final report will be completed within six months from the end of the study period. Extensions for unforeseen circumstances will be handled accordingly.

The study will operate in accordance with the provisions of Public Law 92-463, "Federal Advisory Committee Act," and DoD Instruction 5105.04, "DoD Federal Advisory Committee Management Program." It is not anticipated that this study will need to go into any "particular matters" within the meaning of title 18, United States Code, section 208, nor will it cause any members to be placed in the position of action as a procurement official.

Michael D. Griffin