



CLEARED
For Open Publication

Dec 09, 2019

Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

DEPARTMENT OF DEFENSE DEFENSE SCIENCE BOARD

December 2019



Executive Summary ROLE OF THE DOD IN HOMELAND DEFENSE

OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING

This report is a product of the Defense Science Board (DSB). The DSB is a Federal Advisory Committee established to provide independent advice to the Secretary of Defense. Statements, opinions, conclusions, and recommendations in this report do not necessarily represent the official position of the Department of Defense.



ACQUISITION,
TECHNOLOGY
AND LOGISTICS

THE UNDER SECRETARY OF DEFENSE

3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

OCT 20 2016

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Terms of Reference – Defense Science Board Task Force on the Role of the DoD in Homeland Defense

The decade after 9/11 saw high profile efforts by the U.S. government to address threats to the homeland, focused principally on non-state terrorism and their potential for executing “unconventional” attacks. More recently, the nation has begun pulling back from its military deployments and operations in Iraq and Afghanistan, and efforts at the Department of Homeland Security (DHS) have been rebalanced to improve emergency response and consequence management for natural disasters. In turn, more attention related to national security is being placed on the rise of provocative actions by nation states, such as Russia and China; on the breeding grounds for instability, such as Syria and Ukraine; and on ISIL-inspired threats.

As we learn more about current nation state, pseudo-nation, or non-state capabilities and doctrine, threats to the homeland are re-gaining attention as a serious concern. Motives for attacking the US homeland, besides terrorism, include delaying and disrupting our global projection of armed forces so as to give an adversary state or group time to solidify gains elsewhere, or the belief that the US can be dissuaded or deterred and its will to fight eroded. Adversaries may be “composite” mixes of states and proxies. With advances and availability of technology, their means of attack(s) are broader and may be multiple while targets have become increasingly interdependent as reliance on information technologies has grown.

Addressing homeland security and resiliency, compared to the early 2000s, must take into account this more complex context of multiple nation state and quasi-state competitions, growing sophistication in the exploitation of social media and cyber connectedness, and technology advances that can put the most threatening weapons, including WMD and cyber, into the hands of almost any state or group that desires to possess them. The delivery capabilities for affecting these types of attacks range from the advent of drones to highly sophisticated anonymized or misattributed sources of cyber attacks.

Between 2002 and 2007 the DSB took several looks at the challenges posed by—and preparedness to deal with—threats to the homeland as understood during that time period, especially with respect to DoD roles, missions, and force posture, and how they were or were not well integrated with a maturing DHS. With the significant changes in the threat, environment and technology that have occurred since then, a new assessment should be undertaken, with special attention paid to the nation’s preparedness to deal with a major attack on the homeland.

The DSB is asked to form a task force to assess the current posture of the government and supporting organizations, particularly with respect to the preparedness of DoD to execute its missions, both in the homeland and abroad. The emphasis should be on scoping the challenges

facing DoD in executing its missions. The task force will produce a report of its findings and recommendations. Questions which the study should address include:

- What capabilities (besides an intercontinental missile strike) are other nations or well resourced groups developing that could threaten the homeland across all domains (air, land, maritime, space, cyber). What is the known risk (vulnerability, consequence, threat), assessed ability, likelihood and will to employ them?
- What targets are threatened and how vulnerable are they? Address particularly military (bases and installations, logistics) targets, and their interdependencies.
 - What are the most significant shortfalls for critical government and private-sector organizations that would impact DoD operations in the face of complex threat streams?
- Understand how well prepared partner agencies are in preventing, interdicting, responding to, recovering from, and continuing operations after such an attack, specifically involving significant disruption to support for military operations?
- How well prepared is DoD in its Homeland Defense missions including preventing, interdicting, and responding to an attack?
- What is DoD's priority/readiness for homeland defense, as well as its ability to successfully prosecute an "away game" if critical infrastructure or homeland military capabilities (especially command and control functions) are seriously degraded?
 - In addition to active duty forces, include an assessment of the posture and resourcing of the National Guard and Reserve forces.
 - Are readiness metrics sufficient to provide confidence that DoD can execute its missions, both at home and abroad, in the context of an attack on the homeland?

The study will operate in accordance with the provisions of the Federal Advisory Committee Act (Public Law 92-463) and DoD Directive 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 member to be placed in the position of action as a procurement official.

I will sponsor the study, and Dr. Miriam John and the Honorable Judith Miller will serve as co-chairs. Colonel William Matney will serve as the Executive Secretary and Lt Col Victor Osweiler will be the Defense Science Board Secretariat Representative.

The task force members are granted access to those Department of Defense officials and data necessary for the appropriate conduct of their study. The Under Secretary of Defense for Acquisition, Technology, and Logistics 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 3 months of signing this Terms of Reference and the study period will be between 9 to 12 months. The final report will be completed within 6 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 P.L. 92-463, the "Federal Advisory Committee Act" and DoD Directive 5105.04, the 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 member to be placed in the position of action as a procurement official.

A handwritten signature in dark ink, appearing to read 'Frank Kendall', with a stylized, flowing script.

Frank Kendall

DSB Task Force on the Role of the DoD in Homeland Defense

Membership

Chairs

Dr. Miriam John
Honorable Judith Miller

Honorable Judith Miller
Private Consultant

Members

Dr. Amy Alving
Private Consultant

Dr. Andrew Liepman
RAND

MG Ray Carpenter, USA (Ret.)
Private Consultant

Dr. Joe Markowitz
Private Consultant

Dr. Ruth David
National Academy of Engineering

RADM Steve Metruck, USCG (Ret.)
Executive Director Port of Seattle

Mr. Christopher Day
Cyxtera Technologies

Mr. Kenneth Rapuano¹
*Assistant Secretary of Defense for Homeland
Defense and Global Security*

Mr. William Delaney
*Massachusetts Institute of Technology Lincoln
Laboratory (MIT/LL)*

Mr. Todd Rosenblum
IBM

GEN Chuck Jacoby, USA (Ret.)
Capitol Peak Asset Management

VADM Edward Straw (Ret.)
Osprey Venture Partners

Ambassador James Jeffrey
Private Consultant

Mr. Pete Verga
Department of Defense

Dr. Ronald Kerber
Private Consultant

Ms. Leigh Warner
Private Consultant

¹ Joined administration during Task Force

Government Advisors

Ms. Kelly Brickley
National Counterproliferation Center

Mr. Thomas Janes
Office of the Director of National Intelligence

Mr. Steve Harris
*Department of Homeland Security National
Protection and Programs Directorate*

COL Richard Lebel
U.S. National Guard

Mr. Jan Ithier
NORAD-USNORTHCOM

Mr. Michael Powers
Federal Bureau of Investigation

Col Paul Reedy
Joint Staff/J5

Mr. Jim Stahlman
OASD(HD&GS)

Mr. Robert Salesses
*Office of the Assistant Secretary of Defense for
Homeland Defense and Global Security
(OASD(HD&GS))*

CRD Brian Smicklas
U.S. Coast Guard

Executive Secretary

Colonel William Matney
Air National Guard

DSB Secretariat Representative

Lt Col Victor Osweiler,
United States Air Force

Defense Science Board Secretariat

Mr. Kevin Doxey
Executive Director

Ms. Karen D. H. Saunders
Former Executive Director

Mr. Edward Gliot
Executive Director, Acting

Study Support

Ms. Sarah Gamberini
Former SAIC

Ms. Juliet Fielding
SAIC

DSB Task Force on the Role of the DoD in Homeland Defense

Executive Summary

Over the past several decades, the Department of Defense (DoD) primarily focused on power projection abroad under the assumption that the U.S. homeland was immune to any serious non-nuclear attack(s). That assumption has now been called into question by the *2018 National Defense Strategy Summary*, which states, “It is now undeniable that the homeland is no longer a sanctuary.” Our competitors have become more aggressive and are developing power projection capabilities of their own, coupled with cyber offensive and exploitation operations. In spite of the awareness raised by the *2018 National Defense Strategy* (NDS), the Task Force found that the DoD is currently ill-prepared to deter and defend against these threats to the homeland.

The Task Force was charged with examining threats to the homeland from adversary nations as well as non-state actors across all warfighting domains. Specific areas of investigation included:

- Assessing threats to the homeland and its most vulnerable targets;
- DoD’s posture in its homeland defense mission;
- DoD’s ability to prosecute an overseas contingency if critical infrastructure and military targets based in the homeland are threatened or attacked; and
- Shortfalls and improvements in warning, detection, tracking, and interdiction capabilities against emerging kinetic threats to the nation.

Since WWII the United States has been fortunate not to have faced serious conventional threats to the homeland, but that luck is running out. Attacks against the homeland will most certainly include those on infrastructure and facilities whose loss will impede force projection abroad. Current air and maritime defense capabilities will be seriously challenged against emerging adversary capabilities. Attacks on the electric grid or Defense Critical Infrastructure – both kinetic and digital – could slow down or stall the movement of U.S. forces in other theaters.

Neglecting the defense of the homeland is no longer a luxury that the United States can afford. The DoD must recognize the primacy of its homeland defense mission and respond with a concerted effort to ensure it can fulfill its homeland defense responsibilities. The recommendations of this Task Force provide DoD with the building blocks for doing so by:

- Creating a comprehensive and integrated picture of threats to the homeland;
- Ensuring that NORAD-USNORTHCOM’s initiatives to transition to a warfighting command are supported;

- Partnering with the interagency and private sector owners to ensure the resiliency of infrastructure critical to national security; and
- Addressing air and maritime defense.

Without a well-protected homeland, the United States will struggle to deter great power competitors and defeat peer adversaries. It is imperative that the DoD address the recommendations provided by this Task Force quickly and with the seriousness of purpose that they deserve.