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

RESEARCH
AND ENGINEERING

JUN 1 8 2018

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Terms of Reference - Defense Science Board Task Force on Strengthening Counterintelligence Capabilities Against the 'Insider' Threat

Modern technology has vastly increased the capacity and effectiveness of adversary foreign intelligence organizations to deeply penetrate U.S. civic, commercial, scientific-industrial, and governmental institutions. Ironically, these capabilities have been enabled by the extraordinary functionality for national security missions of modern computer-based capacity to access vast aggregations of sensitive data. The extraordinary functionality of networked storage and processing of data has also created a profound set of vulnerabilities that have been exploited by adversary States as well a non-State entities.

While the valuation of lost intellectual property is difficult to estimate, in 2012, the former Director of the National Security Agency (NSA), GEN Keith Alexander asserted that the economic value of intellectual property from U.S. industry lost to attacks on U.S. computer networks – defense and non-defense to be ~ $1 trillion. The protection of data stored in networks from cyber-attacks from governmental and non-governmental entities ("cyber-security") has become an important preoccupation of both public and private sector investment. However, the U.S. Government's (USG) most damaging loses have been produced by a very small number of 'insiders' entrusted with the protection of these data whose access to huge data sets have produced losses on a staggering scale.

The United States has suffered extensive losses of critical national security data to adversaries. Two of the most spectacular cases recent cases have produced losses of highly classified material on an unprecedented scale; NSA contractors Edward Snowden (1.7 million documents over a brief period) and William T. Martin (>50 terabytes of data stolen over a 20-year period), and U.S. Army Private Manning (750,000 documents stolen over a brief period) illustrate the scale of the problem. The purloined data confers extensive insights into U.S. capabilities that cost hundreds of billions to create, sustain, and protect. USG Counterintelligence (CI) capabilities, while distributed throughout national security institutions, remains law enforcement focused, process-dominated, and full time equivalent-intense. CI institutions operate under processes and authorities designed to engage adversary intelligence collection, many of which were established before networked computers and storage became the dominant repository for sensitive Government data. In this environment, CI mission performance, particularly against the 'insider threat' is unlikely to materially improve simply with additional resources. New approaches to the CI mission need to be considered.

The principal objective of this Task Force is to investigate opportunities to introduce the applications of advanced science and technology (S&T) to enable effective CI initiatives to deter, detect, monitor, and enforce the protection of national security information subject to unauthorized

access or distribution of such information by employees, contractors or other with a plausible claim to legitimate trusted 'insider' access to controlled or classified information. The Task Force should consider three separate but related lines of inquiry:

1. ***Enhancing the ability of CI organizations to identify, track, and locate 'insider' threats***: The application of advanced S&T (e.g., artificial intelligence) to improve the capability of CI organizations to identify and track 'insider' threats to enable the USG to take appropriate measures to protect sensitive data and prevent its loss or compromise, or failing that, to provide insights into 'insider' behavior that produced the loss of data to assure an evidentiary base for effective enforcement measures against such insiders, as well as insights into adversary Tactics, Techniques, and Procedures and tradecraft that will facilitate the future improvement of CI operations.

2. ***Making it more difficult for 'insiders" to steal or divert USG data to unauthorized users***: 'Insider' access to large data sets from Government networks and storage entities is facilitated by the ease with which trusted insiders can acquire, store, and transmit such purloined data to unauthorized users. The problem of protecting such data is not a problem unique to the Federal Government. Commercial entities have employed modern technology to make the theft of sensitive data (e.g., IP, process knowledge) more difficult, and to facilitate detection and tracking of its onward distribution, as well as to make commercial exploitation of stolen data riskier for the user and making it more likely that successful enforcement actions can be undertaken.

3. ***Increasing the cost and risk of adversary governments using non-government advocacy organizations to conceal or obscure their role in the acquisition or exploitation of stolen USG data***: Sensitive USG national security-related information is valuable to foreign intelligence organizations and governments, but also has value to other users in related, and often inter-twined domains. Adversary exploitation of stolen data has been used for diplomatic ends by decoupling the adversary government from its role in the theft of USG data through its distribution to witting or unwitting advocacy groups (e.g., WikiLeaks distribution of the Manning and Snowden documents). In other cases, data (including sources and methods shared with criminal enterprises for unlawful purposes) may be employed for the benefit of both adversary governments and criminal enterprises creating incentives for both.

I will sponsor the study. Dr. William Schneider and Mr. Robert Nesbit will serve as the co-Chairmen of this study. Mr. Michael Dulak, Under Secretary of Defense for Intelligence, will serve as the Executive Secretary. Mr. David Moreau will serve as the Defense Science Board Secretariat representative.

The task force members are granted access to those Department of Defense (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 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 three 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 member to be placed in the position of action as a procurement official.

Michael D. Griffin