DEPARTMENT OF DEFENSE
DEFENSE SCIENCE BOARD

STRENGTHENING COUNTERINTELLIGENCE CAPABILITIES AGAINST THE 'INSIDER' THREAT

August 2020

Executive Summary

OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING

DEFENSE SCIENCE BOARD

OFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301–3140

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING

SUBJECT: Final Report of the Defense Science Board (DSB) Task Force on Strengthening Counterintelligence Capabilities Against the "Insider" Threat

I am pleased to forward the final report of the Defense Science Board Task Force on Strengthening Counterintelligence Capabilities Against the "Insider" Threat, co-chaired by Dr. William Schneider and Mr. Robert Nesbit.

After the attacks of September 11, 2001, counterintelligence resources were diverted to address the urgent threats posed by terrorist organizations. For almost two decades, the counterintelligence mission has not received the sustained and focused attention that it needs to protect the nation from stand-alone actors or actors working under the direction of a foreign intelligence service. The damage that such actors can cause to U.S. national security has grown substantially as classified information is increasingly stored on computers, making more of it available to retrieve and easier to spread. Peer competitors have made a concerted effort to access classified and business proprietary information, either to thwart U.S. national security objectives or to advance their own military and civil sectors. It is long past time for the United States to address the insider threat and reduce damage caused by leaked or stolen national security information.

I endorse the findings of this report and believe its recommendation offer a sound starting point for assessing new technologies and techniques to deter and defeat insider threats. The Department of Defense should view this report as a call to action and respond accordingly.

Eric D. Evans

Dr. Eric D. Evans
Chairman, Defense Science Board

THIS PAGE LEFT INTENTIONALLY BLANK

DEFENSE SCIENCE BOARD

OFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301–3140

MEMORANDUM TO THE CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Final Report of the Defense Science Board (DSB) Task Force on Strengthening Counterintelligence Capabilities Against the "Insider" Threat

Attached is the final report of the Defense Science Board Task Force on Strengthening Counterintelligence Capabilities Against the "Insider" Threat. The Task Force surveyed the large and growing problem of individuals working for or with the U.S. government leaking or stealing national security information, either alone or at the direction of a foreign intelligence service. Specifically, the Task Force investigated new technologies and creative measures for securing classified information, deterring and preventing theft, and identifying individuals who may be untrustworthy.

There are a number of new tools that, if adopted, will make stealing classified information more difficult for insiders, and will help counterintelligence officials identify dangerous individuals before – not after – the compromise of national security. The Task Force recommends further study and adoption of these tools, including behavioral analysis, advanced network monitoring, and digital watermarking of physical and digital documents.

Just as the Task Force was completing its work, the President issued the National Counterintelligence Strategy for 2020-2022. As he wrote, "The Nation faces an expanding array of foreign intelligence threats by adversaries who are using increasingly sophisticated methods to harm the United States… [preserving] peace and security [requires] going on the offense against aggressive foreign intelligence services that work against democracy, United States allies, and our national security priorities."

We believe that this report is a timely wake-up call to the Department of Defense and the Intelligence Community about the nature and danger of foreign intelligence threats, and that the recommendations included herein should be quickly adopted.

Mr. Robert Nesbit
Task Force Co-Chair

Dr. William Schneider
Task Force Co-Chair

THIS PAGE LEFT INTENTIONALLY BLANK

Executive Summary of the DSB Report on Strengthening Counterintelligence Capabilities Against the 'Insider' Threat

Table of Contents

Executive Summary

Task Force Bottom Line

The insider threat[1] would not be so formidable were it not for the outsider threat. Yet counterintelligence (CI) operations continue to focus on a case-by-case approach with a strong law enforcement emphasis in dealing with escalating foreign intelligence threats. National CI resources (with a few noteworthy exceptions) are concentrated within the United States rather than engaging the foreign intelligence services abroad, thus ceding an advantage to the adversary.

A more creative—and potentially effective—approach would integrate proactive counterintelligence operations into national security strategy and planning. The purpose would be twofold: 1) to develop an understanding of foreign intelligence organizations, motives, targets, tools, and vulnerabilities; and 2) to develop policy options to weaken the adversary's intelligence enterprise as U.S. national security objectives might dictate.

Summary of Key Judgments

- Without actionable intelligence insights into adversary intelligence activities, the DoD will continue to be at a severe disadvantage in identifying and containing insider threats.
- DoD CI components are in need of a major technology upgrade in their operational toolsets and advanced data processing applications.
- Overall progress in the 44 DoD components and agencies is quite slow as measured by progress in meeting national and department minimum standards for insider threats.
- A significant number of costly compromises resulted from insiders circumventing the security on classified DoD and intelligence community (IC) networks with relative ease. Despite lessons learned from high profile insider cases, well established and high priority security controls continue to be absent or are malfunctioning. It is difficult to imagine a good excuse for this neglect.

Summary of Recommendations

- **Recommendation 1:** This recommendation is UNCLASSIFIED//For Official Use Only. See final report for more information.
- **Recommendation 2: Risk Rating** – The DoD Insider Threat Program Office should work with the 44 components and agencies within the DoD to enable a broader, standardized, and more cost-effective application of risk rating tools (RRT).

[1] As used herein, "insider threat" means we recognize there are broader insider threat concerns (e.g., terrorism, workplace violence) but our Task Force on Counterintelligence has not been tasked to look at the broader issues.

- Move ahead much faster with implementing a risk rating tool.
  - Begin by getting consensus on what data will be used and what data should not be used.
  - Prioritize rating employees with access to the most sensitive data.
- Where funding for the UAM portion of the tool is holding up progress, examine less expensive so-called 80% solutions

- **Recommendation 3: IT Security –** Defense Counterintelligence and Security Agency (DCSA) should work with the DoD Chief Information Officer (CIO) and Chief Information Security Officer (CISO) to improve the security apparatus which also serves as a *de facto* "sensor array" for the CI function.
- **Recommendation 4: S&T** – Under Secretary of Defense for Intelligence and Security (USD(I&S)) and Under Secretary of Defense for Research and Engineering (USD(R&E)) should jointly explore ways to exploit existing science and technology (S&T) to improve DoD CI.

Technical Path Forward Opportunities

The following opportunities are based on the analysis of the Task Force during the year-long study. Some of these points are independent of one another, and hence are additive rather than mutually exclusive in their use supporting the security and CI missions. The following are among the most promising opportunities:

(1) **Improve counterintelligence capabilities and tools to identify and disrupt foreign intelligence operations that employ insiders to support their goals.**

   a. Prioritize proactive CI collection and analysis;

   b. Exploit existing S&T investments to improve CI tools and capabilities, including:

      i. Advertising technology (AdTech), and

      ii. Advances in facial recognition technology.

(2) **Devise improved capabilities and tools to identify and apprehend stand-alone actors seeking to steal, disrupt, subvert, or sabotage DoD information and systems.**

   a. Leverage civil sector experience to develop appropriate risk-rating tools to facilitate the cost-effective allocation of security and CI resources to the mission.

   b. Develop applications of digital watermarking to enhance deterrence and facilitate enduing accountability for access to DoD information (electronic or physical) and objects.

(3) **Make it more difficult for malevolent DoD insiders to steal, modify or divert classified or export-controlled information to unauthorized users.**

a. Implement basic cyber controls throughout the DoD information enterprise that contains classified or export-controlled information.

b. Encrypt classified and export-controlled data in all removable media and mobile devices.

c. Examine opportunities for the use of virtualization technology that could contribute in a cost-effective manner to the security of classified and export-controlled information.

(4) **Reduce the adversary's confidence in the value and validity of any stolen information.**

a. Adapt and expand the use of data obfuscation technology.

(5) **Establish a program to continuously infuse technical upgrades into CI operational toolsets and data processing capabilities.**

Appendix A: Task Force Terms of Reference

RESEARCH
AND ENGINEERING

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

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

Appendix B: Task Force Membership

Co-Chairs

Mr. Robert Nesbit
Private Consultant

Dr. William Schneider
International Planning Services

Members

Mr. Nicholas Eftimiades
Pennsylvania State University

Mr. James Gosler
Johns Hopkins Applied Physics Laboratory

Mr. Alfred Grasso
The MITRE Corporation

Mr. Richard Haver
Private Consultant

Mr. Lincoln Leibner
Logos Technologies

Dr. Joseph Markowitz
Private Consultant

Ms. Lori Scherer
The MITRE Corporation

Mr. Randy Trzeciak
Carnegie Mellon University

Ms. Michelle Van Cleave
Private Consultant

Mr. Vincent Vitto
Private Consultant

Government Advisors

Mr. John Dixson
Defense Intelligence Agency

Special Agent Nancy Kurokawa
Naval Criminal Investigative Service

Mr. Mark Dupont
Army Intelligence & Security Command

Mr. Daniel Persson
Air Force Office of Special Investigations

Mr. Robert Giesler
Office of the Secretary of Defense

Mr. William Stephens
Defense Counterintelligence & Security Agency

Executive Secretary

Mr. Michael Dulak
Office of the Under Secretary of Defense for Intelligence and Security

Defense Science Board Secretariat

Mr. Kevin Doxey
Executive Director

Lt Col Milo Hyde IV, USAF, Ph.D.
Designated Federal Officer

Study Support

Ms. Clare Mernagh
SAIC

Ms. Brenda Poole
SAIC

Appendix C: Briefings Received

9-10 January 2019 Meeting

Ethics Briefing and DSB Secretariat Remarks
DoD General Counsel and DSB Secretariat

Insider Threat Investigation and Arrest
Federal Bureau of Investigation

Insider Threat Perspective
Defense Intelligence Agency

Threat and Investigation
U.S. Army Intelligence and Security Command

Factor 8 Program, Threat/Solutions of Non-Traditional Collectors
Open Source Enterprise

StormSystem
Office of the Secretary of Defense, Strategic Capabilities Office

Threat Overview
Defense Intelligence Agency

13-14 February 2019 Meeting

DoD Insider Threat Program
Office of the Under Secretary of Defense for Intelligence and Security

DoD Counterintelligence
Office of the Under Secretary of Defense for Intelligence and Security

Defense Insider Threat Management and Analysis Center (DITMAC)
DITMAC

Air Force Insider Threat Program (AFInTP)
AFInTP

Army Insider Threat Program
Army Protection Directorate

Missile Defense Agency Insider Threat
Missile Defense Agency

Current and Upcoming Credible Assessment Technologies
National Center for Credibility Assessment

Human Behavior and Cybersecurity
MITRE

NCIS Insider Threat Division
Naval Criminal Investigative Service

National Counterintelligence Strategy
Task Force Member

6-7 March 2019 Meeting

SquirrelWERKZ Tools
SquirrelWERKZ

Army User Activity Monitoring Program
U.S. Army Cyber Command

NSA Insider Threat Program
National Security Agency

Thomson Reuters Special Services
Thomson Reuters

Corporate Risk Tools
Lockheed Martin Corporation

Forcepoint Platform
Forcepoint

Wells Fargo
Wells Fargo

Splunk
Splunk, Inc.

CIA Enterprise Insider Threat Program
Central Intelligence Agency

10-11 April 2019 Meeting

Chinese Economic Espionage
Task Force Member

Social Media and Online Activity Profiles
Defense Technology Integration Program Office

Threat and Investigation
Air Force Office of Special Investigations

Digital Guardian Platform
Digital Guardian

Mercury Systems
Mercury Systems, Inc.

Booz Allen Hamilton
Booz Allen Hamilton

21-22 May 2019 Meeting

Threat Response and Supply Chain Security
MITRE

DoD Offensive Counterintelligence Operations
Naval Criminal Investigative Service
Defense Intelligence Agency
Office of the Under Secretary of Defense for Intelligence and Security

Media Forensic Program
Defense Advanced Research Projects Agency

Defense Personnel and Security Research Center (PERSEREC)
PERSEREC

Marine Corps Insider Threat Program
Headquarters Marine Corps

National Insder Threat Task Force
National Counterintelligence and Security Center

19-20 June 2019 Meeting

Question and Answer Session
Office of the Under Secretary of Defense for Intelligence and Security

Digital Watermarking
Henrae LLC and Digimarc

9 July 2019 Meeting

Digital Watermarking
Naval Criminal Investigative Service

18-19 September 2019 Meeting

DIA Country-Specific Analysts
Defense Intelligence Agency

Counterintelligence Techniques
Central Intelligence Agency

Remote Risk Assessment Tool
AC Global Risk

"GoSilent" Technology
Attila Security

2-3 October 2019 Meeting

Assured Identity Initiative
Defense Information Systems Agency

Threat Briefing
National Intelligence Council

Defense Counterintelligence and Security Agency
Defense Counterintelligence and Security Agency

National Threat Identification and Prioritization Assessment
Office of the Director of National Intelligence

Appendix D: Acronyms and Abbreviated Terms

AdTech	advertising technology
CI	Counterintelligence
CISO	chief information security officer
DCSA	Defense Counterintelligence and Security Agency
DoD	Department of Defense
FFRDC	federally funded research and development center
OSD	Office of the Secretary of Defense
S&T	science & technology
UARC	university affiliated research center
USD(I&S)	Under Secretary of Defense for Intelligence and Security
USD(R&E)	Under Secretary of Defense for Research and Engineering