DoD's Research Security and S&T Protection Efforts to Counter Foreign Influence

PRESENTED BY:

Mr. Kristopher Gardner

Director, S&T Protection, STP&E

Office of the Under Secretary of Defense for Research and Engineering

MODERATED BY:

Steve Redifer

2021-05-13

HDIAC
Homeland Defense & Security
Information Analysis Center

HDIAC is sponsored by the Defense Technical Information Center (DTIC). Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Defense Technical Information Center. DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited.

info@hdiac.org
https://www.hdiac.org

Strategic Technology Protection and Exploitation (STP&E) Science and Technology (S&T) Protection Efforts

Kristopher Gardner
Director, S&T Protection, STP&E
Office of the Under Secretary of Defense
for Research and Engineering

Homeland Defense Information Analysis Center
May 13, 2021

https://www.CTO.mil *@DoDCTO*

Agenda

- Strategic Context
- STP&E S&T Protection Efforts
- Q&A

Strategic Context

DoD Strategic Context

- Rapid technological change
- Adversary challenges in every domain
- Preserving technology advantage from diversion, exploitation, and unwanted transfer
- Global competition for talent
- Long-term investment challenges
- Need for rapid technology development and rapid transition

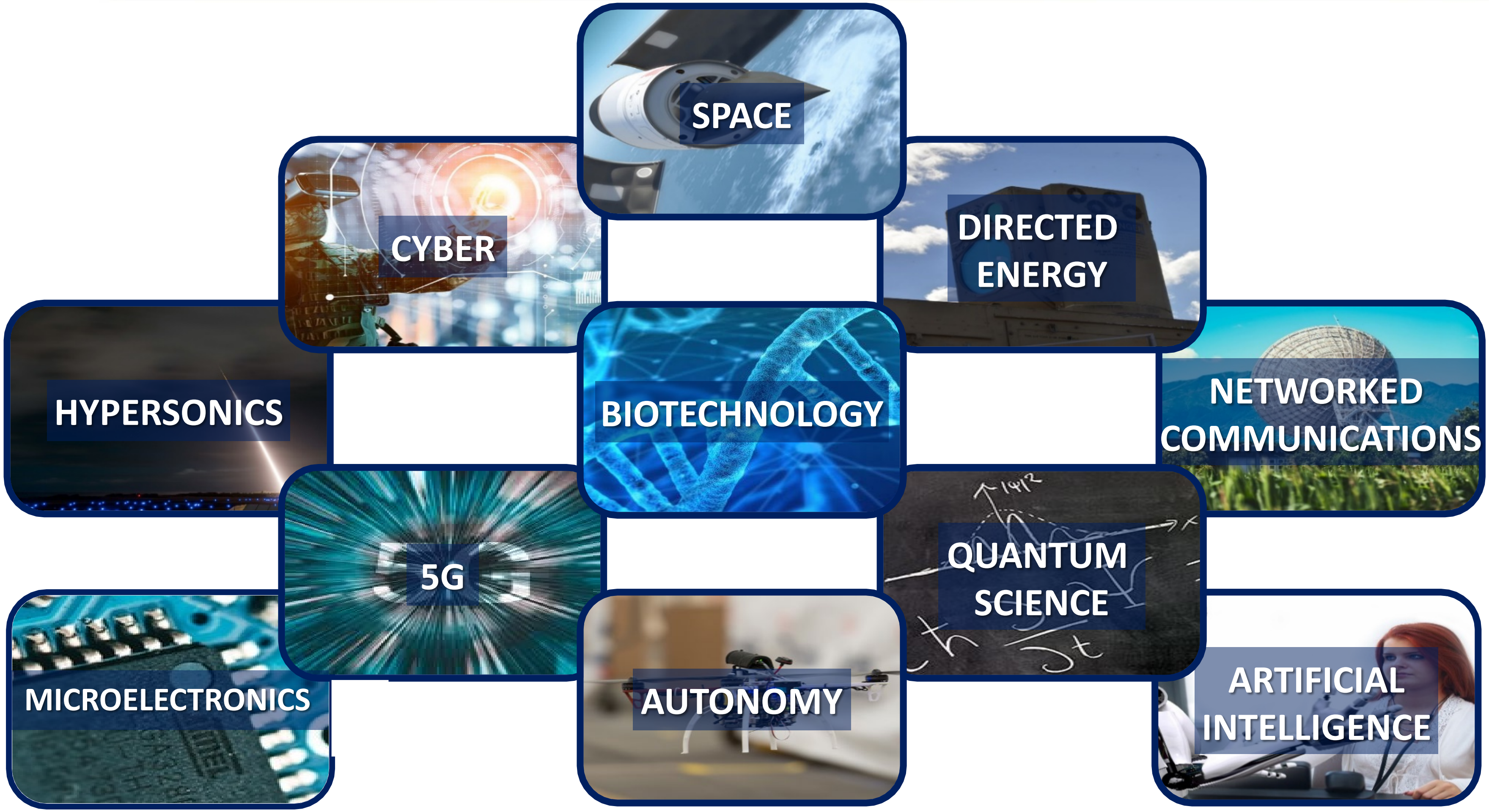
National Defense Strategy

Build a More Lethal Force

Strengthen Alliances and Attract New Partners

Change the Way We Do Business

DoD Modernization Priorities



SPACE

CYBER

DIRECTED ENERGY

HYPERSONICS

BIOTECHNOLOGY

NETWORKED COMMUNICATIONS

5G

QUANTUM SCIENCE

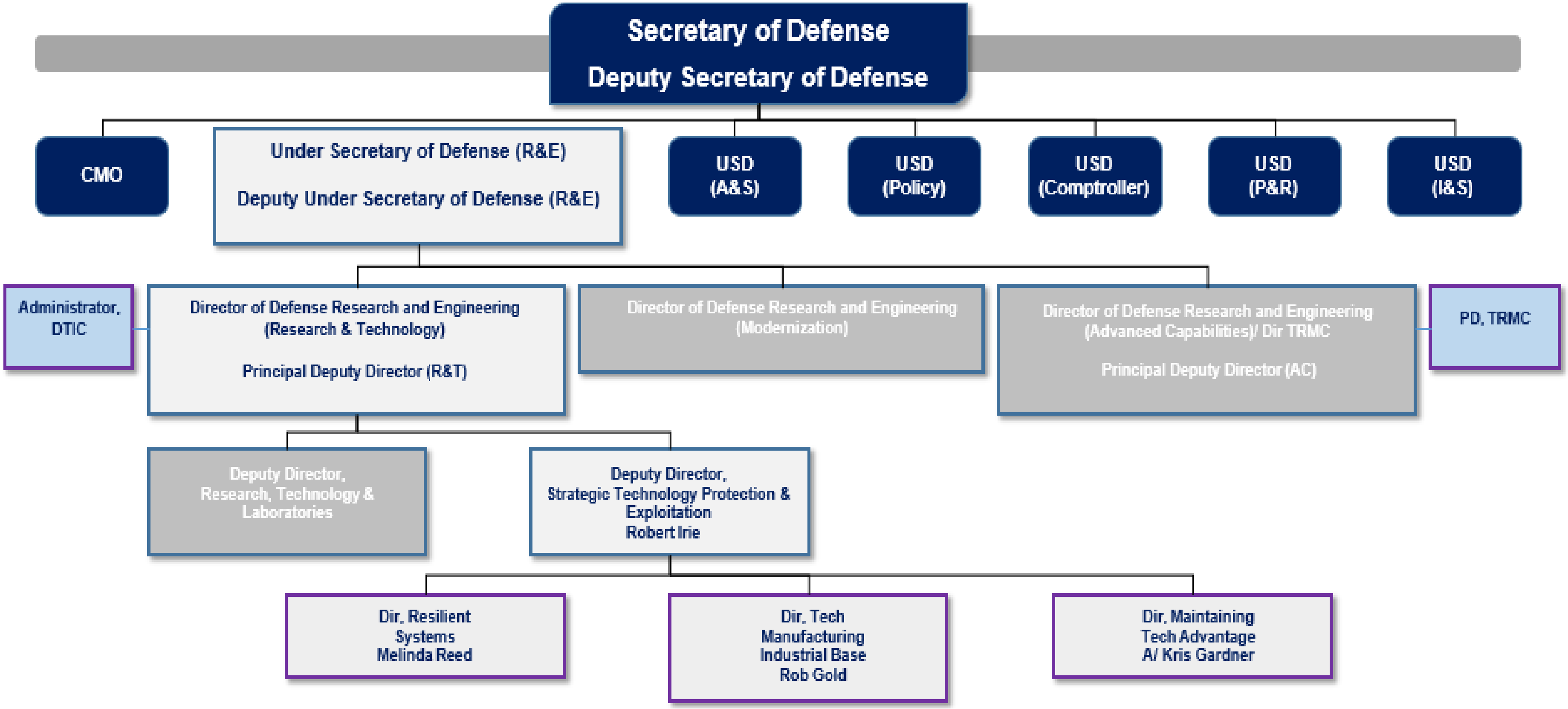
MICROELECTRONICS

AUTONOMY

ARTIFICIAL INTELLIGENCE

These modernization priority areas magnify the Department's technical dominance and support the objectives set forth by the Secretary of Defense and the National Defense Strategy.

OUSD(R&E) in DoD



Secretary of Defense

Deputy Secretary of Defense

CMO

Under Secretary of Defense (R&E)

Deputy Under Secretary of Defense (R&E)

USD (A&S)

USD (Policy)

USD (Comptroller)

USD (P&R)

USD (I&S)

Administrator, DTIC

Director of Defense Research and Engineering (Research & Technology)

Principal Deputy Director (R&T)

Director of Defense Research and Engineering (Modernization)

Director of Defense Research and Engineering (Advanced Capabilities)/ Dir TRMC

Principal Deputy Director (AC)

PD, TRMC

Deputy Director, Research, Technology & Laboratories

Deputy Director, Strategic Technology Protection & Exploitation Robert Irie

Dir, Resilient Systems Melinda Reed

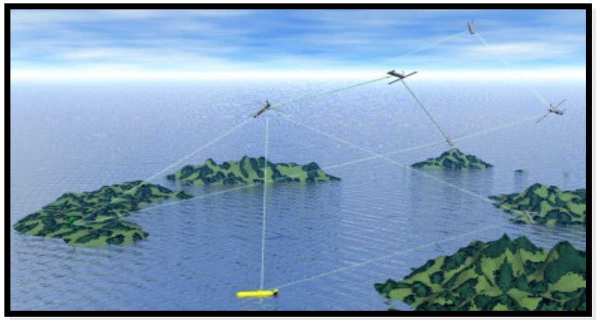
Dir, Tech Manufacturing Industrial Base Rob Gold

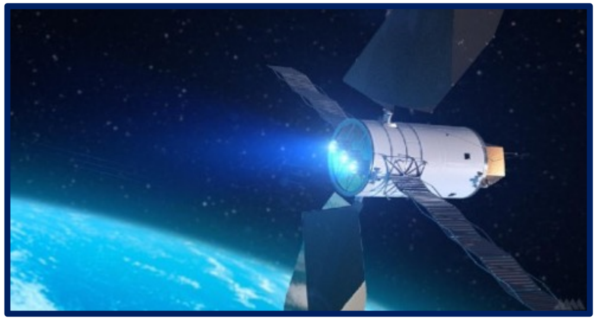
Dir, Maintaining Tech Advantage A/ Kris Gardner

Distribution Statement A: Approved for public release. DOPSR case #21-S-0995 applies. Distribution is unlimited.

Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)) Mission

- **Ensure Technological Superiority for the U.S. Military**
  - Set the technical direction for the Department of Defense (DoD)
  - Champion and pursue new capabilities, concepts, and prototyping activities throughout DoD research and development enterprise
- **Bolster Modernization**
  - Pilot new acquisition pathways and concepts of operation
  - Accelerate capabilities to the Warfighter





Distribution Statement A: Approved for public release. DOPSR case #20-S-2038 applies. Distribution is unlimited.

Strategic Technology Protection & Exploitation Mission and Organization

Deputy Director
Strategic Technology Protection & Exploitation (STP&E)
Dr. Robert Irie

Acting D, Maintaining Technology Advantage
Mr. Kristopher Gardner

D, Resilient Systems
Ms. Melinda Reed

D, Technology and Manufacturing Industrial Base
Mr. Robert Gold

Maintain Leadership in Critical Technology Modernization Areas

- Implement new procedures for Technology Area Protection
- Update DoD and Government-wide procedures to strengthen U.S. research enterprise
- Mitigate exploitation in academia, labs, FFRDCs, and UARCs
- Focus security, counterintelligence, and law enforcement actions to deter adversaries

Foster Assured Resilient Missions, Systems and Components

- Set the technical and policy direction for technology and program protection
- Grow DoD capability/capacity to evaluate and mitigate software component vulnerabilities
- Establish secure cyber resilient weapons, engineering methods and workforce competency

Advance Domestic Innovation Base to Deliver Modernization Goals

- Assess and monitor emerging technology, workforce, engineering, test, & infrastructure base
- Facilitate USG mechanisms and tools to close gaps, foster enabling domestic technology development and manufacturing capability, and counter strategic competitor actions
- Manage the OSD Manufacturing Technology program and Manufacturing Innovation Institutes

MISSION: Promote and protect technology advantage and counter unwanted technology transfer to ensure Warfighter dominance through superior, assured, and resilient systems, and a healthy viable national security innovation base.

STP&E FY21 Activities

- Transform Program Protection methods and practices; enable transition of S&T protections
- Establish Software Assurance Flyaway Teams and modernize Joint Federated Assurance Center capabilities
- Lead secure cyber resilient engineering standards and methods
- Refine Technology Area Protection Plans and conduct outreach
- Engage allies and partners with promote, protect, and counter activities
- Counter strategic competitor exploitation of S&T through Foreign Talent Recruitment Plans
- Identify and assess gaps in emerging technology industry, workforce, and infrastructure base to ensure a smooth and rapid transition from research to fieldable capability for the modernization priorities
- Develop innovation base promote/protect strategies; process technology-related CFIUS and export control cases
- Develop and transition new manufacturing technologies; implement a new institute for synthetic biology and a strategic management approach for the Manufacturing Innovation Institutes; mature a Defense manufacturing human capital strategy

STP&E S&T Protection Efforts

Why Is S&T Protection Necessary?

National Strategy for Critical and Emerging Technologies

November 2020

Great Power Competition

- Russia "is targeting United States technology through the employment of a variety of licit and illicit technology transfer mechanisms to support national-level efforts, including its military and intelligence programs. These actions include using illicit procurement networks, seeking technology transfer through joint ventures with Western companies, and requiring access to source code from technology companies seeking to sell their products in Russia."
- The People's Republic of China is "targeting sources of United States and allied strength by employing means that include stealing technology, coercing companies to disclose intellectual property, undercutting free and fair markets, failing to provide reciprocal access in research and development (R&D) projects, and promoting authoritarian practices that run counter to democratic values."

Maintaining U.S. Technological Advantage

- DoD's Science and Technology (S&T) community, along with the defense industry and research enterprise, will maintain U.S. "leadership Critical and Emerging Technologies by promoting our National Security Innovation Base (NSIB) and protecting our technology advantage."

DoD-Sponsored Research Policy Activities

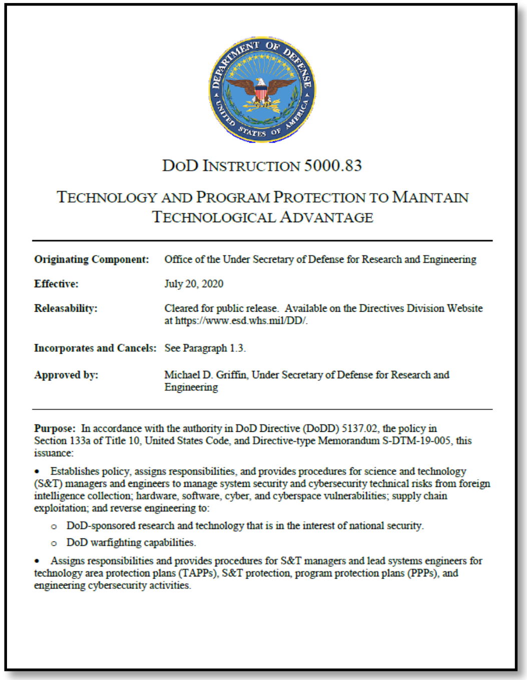
- Department of Defense June 29, 2020 USD(R&E) Memo, "Collecting Assistance Award Information As Required in Section 1281(d)(1) of the National Defense Authorization Act for Fiscal Year 2020," requires at least **annual reporting** of "Participants and Other Collaborating Organizations" **for all individuals participating** in DoD research.

- Instruction (DoDI) 5000.83, "Technology and Program Protections to Maintain Technological Advantage," includes requirement to **evaluate all research programs** for the **appropriateness of funding category** prior to program approval.

- Implementation guidance under development:
  - Pursuing a **standardized risk methodology** for S&T Program Managers to integrate into funding and award decisions.
  - Developing a methodology to make unwanted Foreign Talent Recruitment Program (FTRP) and participant data accessible by all S&T stakeholders in order to **identify and mitigate recruitment and retention activities by adversary talent recruitment programs.**

Collaborating with research and technology protection stakeholders across DoD

Technology, S&T, and Program Protection Planning



DoD Instruction 5000.83

Technology and Program Protection to Maintain Technological Advantage

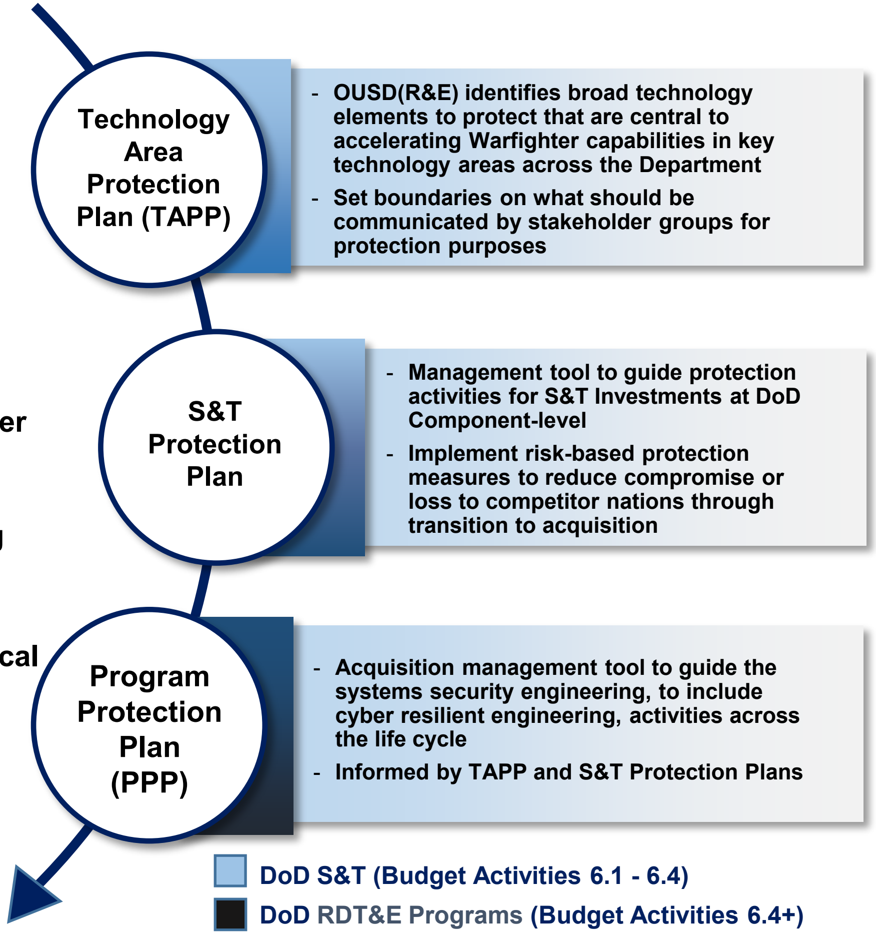
Originating Component:	Office of the Under Secretary of Defense for Research and Engineering
Effective:	July 20, 2020
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Incorporates and Cancels:	See Paragraph 1.3.
Approved by:	Michael D. Griffin, Under Secretary of Defense for Research and Engineering

Purpose: In accordance with the authority in DoD Directive (DoDD) 5137.02, the policy in Section 133a of Title 10, United States Code, and Directive-type Memorandum S-DTM-19-005, this issuance:

- Establishes policy, assigns responsibilities, and provides procedures for science and technology (S&T) managers and engineers to manage system security and cybersecurity technical risks from foreign intelligence collection; hardware, software, cyber, and cyberspace vulnerabilities; supply chain exploitation; and reverse engineering to:
  - DoD-sponsored research and technology that is in the interest of national security.
  - DoD warfighting capabilities.
- Assigns responsibilities and provides procedures for S&T managers and lead systems engineers for technology area protection plans (TAPPs), S&T protection, program protection plans (PPPs), and engineering cybersecurity activities.

Main Content

- Safeguard information
- Control DoD-sponsored research
- Design for security and cyber resiliency
- Protect the system against cyber attacks from enabling and supporting systems
- Protect fielded systems
- Enhance protection for critical programs and technologies



Technology Area Protection Plan (TAPP)

- OUSD(R&E) identifies broad technology elements to protect that are central to accelerating Warfighter capabilities in key technology areas across the Department
- Set boundaries on what should be communicated by stakeholder groups for protection purposes

S&T Protection Plan

- Management tool to guide protection activities for S&T Investments at DoD Component-level
- Implement risk-based protection measures to reduce compromise or loss to competitor nations through transition to acquisition

Program Protection Plan (PPP)

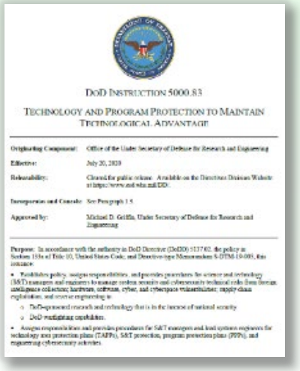
- Acquisition management tool to guide the systems security engineering, to include cyber resilient engineering, activities across the life cycle
- Informed by TAPP and S&T Protection Plans

DoD S&T (Budget Activities 6.1 - 6.4)
DoD RDT&E Programs (Budget Activities 6.4+)

Manage risk of adversarial exploitation and compromise beginning with early S&T and continues through the Acquisition lifecycle

S&T Protection Policy and Guidance Overview

Policy



DoD Instruction 5000.83

Technology and Program Protection to Maintain Technological Advantage

Originating Component: Office of the Under Secretary of Defense for Research and Engineering

Effective: July 20, 2020

Releasability: Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.

Incorporates and Cancels: See Paragraph 1.5

Approved by: Michael D. Griffin, Under Secretary of Defense for Research and Engineering

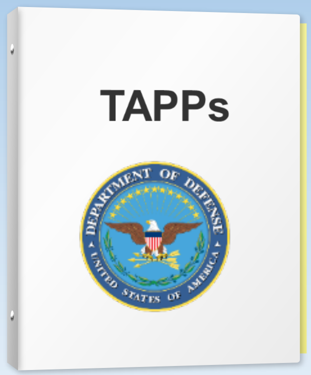
Purpose: In accordance with the authority in DoD Directive (DoDD) 5137.02, the policy in Section 133a of Title 10, United States Code, and Directive-type Memorandum 5-DTM-19-005, this issuance:

- Establishes policy, assigns responsibilities, and provides procedures for science and technology (S&T) managers and engineers to manage system security and cybersecurity technical risks from foreign intelligence collection; hardware, software, cyber, and cyberspace vulnerabilities; supply chain exploitation; and reverse engineering to:
  - DoD-sponsored research and technology that is in the interest of national security.
  - DoD warfighting capabilities.
- Assigns responsibilities and provides procedures for S&T managers and lead systems engineers for technology area protection plans (TAPPs), S&T protection, program protection plans (PPPs), and engineering cybersecurity activities.

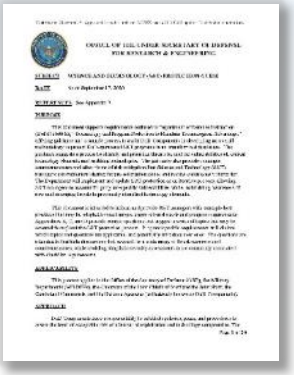
DoDI 5000.83 – Published July 20, 2020

Implemented Through

Guidance



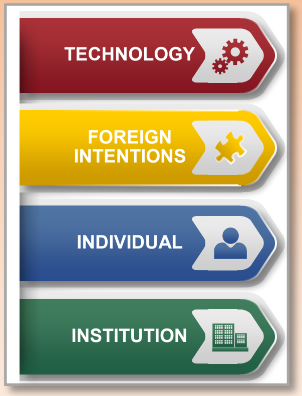
Technology Area Protection Plans – Published 2020-2021



S&T Protection Guide – DRAFT

Supports Adoption of

Templates and Tools



Detailed Risk Assessment (Grants) - DRAFT

Detailed Risk Assessment Tool (In Development)

S&T Protection Plan Template - DRAFT

DoD Components with Templates in Development:

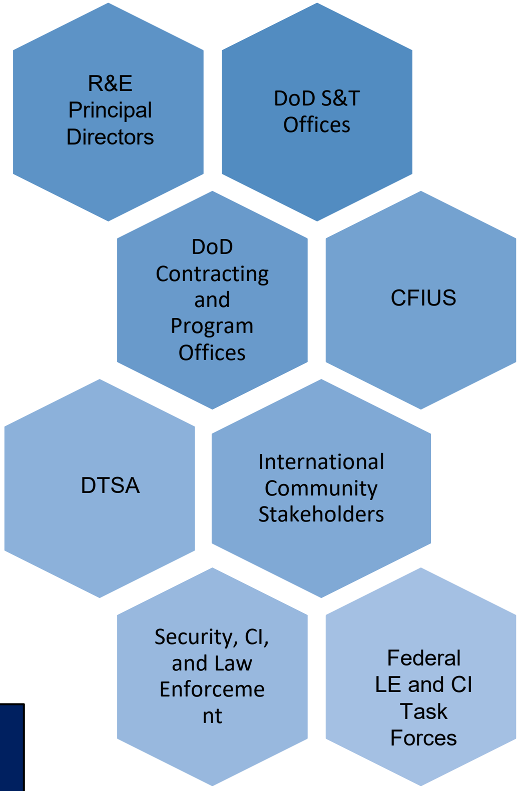
- DARPA
- Army
- Air Force
- Navy
- MDA

Distribution Statement A: Approved for public release. DOPSR case #21-S-1241 applies. Distribution is unlimited.

Technology Area Protection Plan Stakeholders

- Established by USD(R&E) to provide horizontal protection guidance for technology modernization priorities
  - Documents Department-wide messaging guidance
  - Identifies and informs international engagement opportunities
  - Provides focus for counterintelligence, security and law enforcement activities
  - Creates opportunities for open research and collaboration by identifying what requires protection
  - Provides provenance for protecting technologies in acquisition programs
- Shared with Federal interagency partners to inform federal guidelines and consistent implementation

Customers & Stakeholders



R&E Principal Directors

DoD S&T Offices

DoD Contracting and Program Offices

CFIUS

DTSA

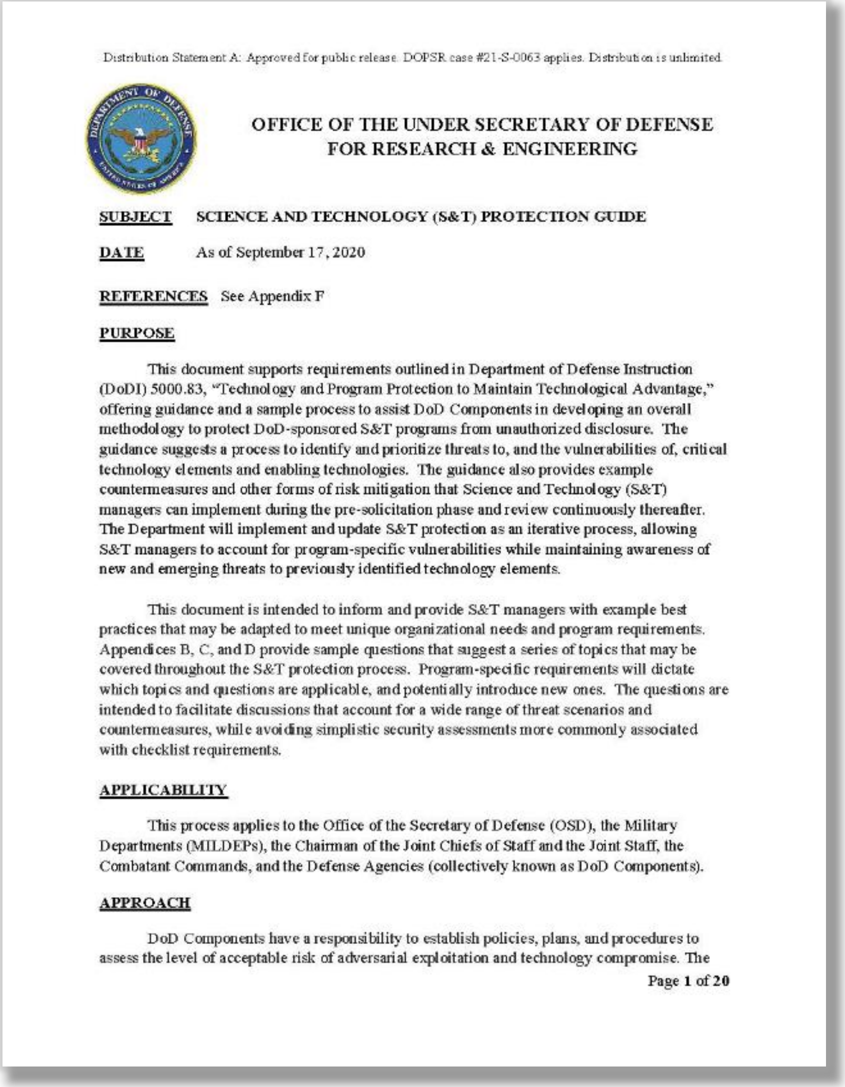
International Community Stakeholders

Security, CI, and Law Enforceme nt

Federal LE and CI Task Forces

Provides consistent protection priorities and messaging across diverse stakeholders

S&T Protection Guide



Distribution Statement A: Approved for public release. DOPSR case #21-S-0063 applies. Distribution is unlimited.

OFFICE OF THE UNDER SECRETARY OF DEFENSE
FOR RESEARCH & ENGINEERING

SUBJECT SCIENCE AND TECHNOLOGY (S&T) PROTECTION GUIDE

DATE As of September 17, 2020

REFERENCES See Appendix F

PURPOSE

This document supports requirements outlined in Department of Defense Instruction (DoDI) 5000.83, "Technology and Program Protection to Maintain Technological Advantage," offering guidance and a sample process to assist DoD Components in developing an overall methodology to protect DoD-sponsored S&T programs from unauthorized disclosure. The guidance suggests a process to identify and prioritize threats to, and the vulnerabilities of, critical technology elements and enabling technologies. The guidance also provides example countermeasures and other forms of risk mitigation that Science and Technology (S&T) managers can implement during the pre-solicitation phase and review continuously thereafter. The Department will implement and update S&T protection as an iterative process, allowing S&T managers to account for program-specific vulnerabilities while maintaining awareness of new and emerging threats to previously identified technology elements.

This document is intended to inform and provide S&T managers with example best practices that may be adapted to meet unique organizational needs and program requirements. Appendices B, C, and D provide sample questions that suggest a series of topics that may be covered throughout the S&T protection process. Program-specific requirements will dictate which topics and questions are applicable, and potentially introduce new ones. The questions are intended to facilitate discussions that account for a wide range of threat scenarios and countermeasures, while avoiding simplistic security assessments more commonly associated with checklist requirements.

APPLICABILITY

This process applies to the Office of the Secretary of Defense (OSD), the Military Departments (MILDEPs), the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, and the Defense Agencies (collectively known as DoD Components).

APPROACH

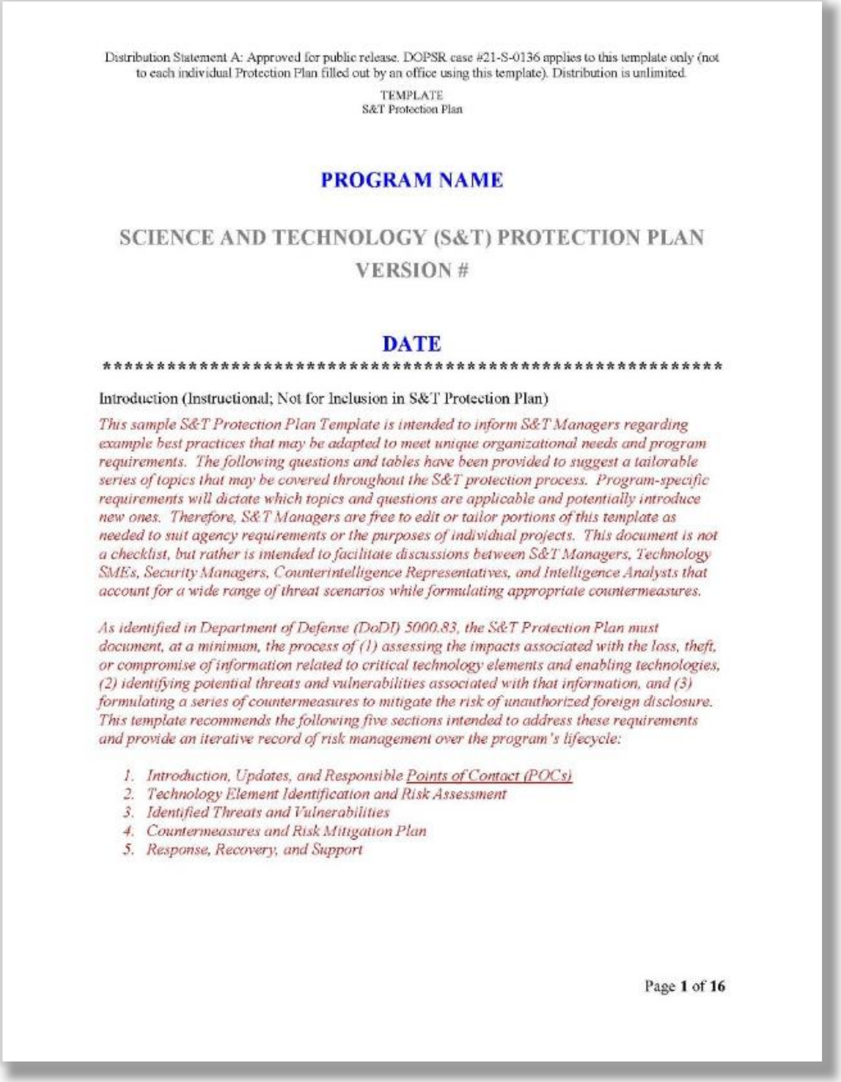
DoD Components have a responsibility to establish policies, plans, and procedures to assess the level of acceptable risk of adversarial exploitation and technology compromise. The

Page 1 of 20

The S&T Protection Guide:

- Offers a sample process to assist DoD Components in developing an overall methodology to protect DoD-sponsored S&T programs from unauthorized disclosure
- Suggests a process to identify and prioritize threats to, and the vulnerabilities of, critical technology elements and enabling technologies
- Provides countermeasures and other forms of risk mitigation to be implemented during the pre-solicitation phase and reviewed continuously thereafter
- Informs S&T managers of best practices that may be adapted to meet unique organizational needs and program requirements

S&T Protection Plan Template



Distribution Statement A: Approved for public release. DOPSR case #21-S-0136 applies to this template only (not to each individual Protection Plan filled out by an office using this template). Distribution is unlimited.

TEMPLATE
S&T Protection Plan

PROGRAM NAME

SCIENCE AND TECHNOLOGY (S&T) PROTECTION PLAN
VERSION #

DATE

****

Introduction (Instructional; Not for Inclusion in S&T Protection Plan)

This sample S&T Protection Plan Template is intended to inform S&T Managers regarding example best practices that may be adapted to meet unique organizational needs and program requirements. The following questions and tables have been provided to suggest a tailorable series of topics that may be covered throughout the S&T protection process. Program-specific requirements will dictate which topics and questions are applicable and potentially introduce new ones. Therefore, S&T Managers are free to edit or tailor portions of this template as needed to suit agency requirements or the purposes of individual projects. This document is not a checklist, but rather is intended to facilitate discussions between S&T Managers, Technology SMEs, Security Managers, Counterintelligence Representatives, and Intelligence Analysts that account for a wide range of threat scenarios while formulating appropriate countermeasures.

As identified in Department of Defense (DoDI) 5000.83, the S&T Protection Plan must document, at a minimum, the process of (1) assessing the impacts associated with the loss, theft, or compromise of information related to critical technology elements and enabling technologies, (2) identifying potential threats and vulnerabilities associated with that information, and (3) formulating a series of countermeasures to mitigate the risk of unauthorized foreign disclosure. This template recommends the following five sections intended to address these requirements and provide an iterative record of risk management over the program's lifecycle:

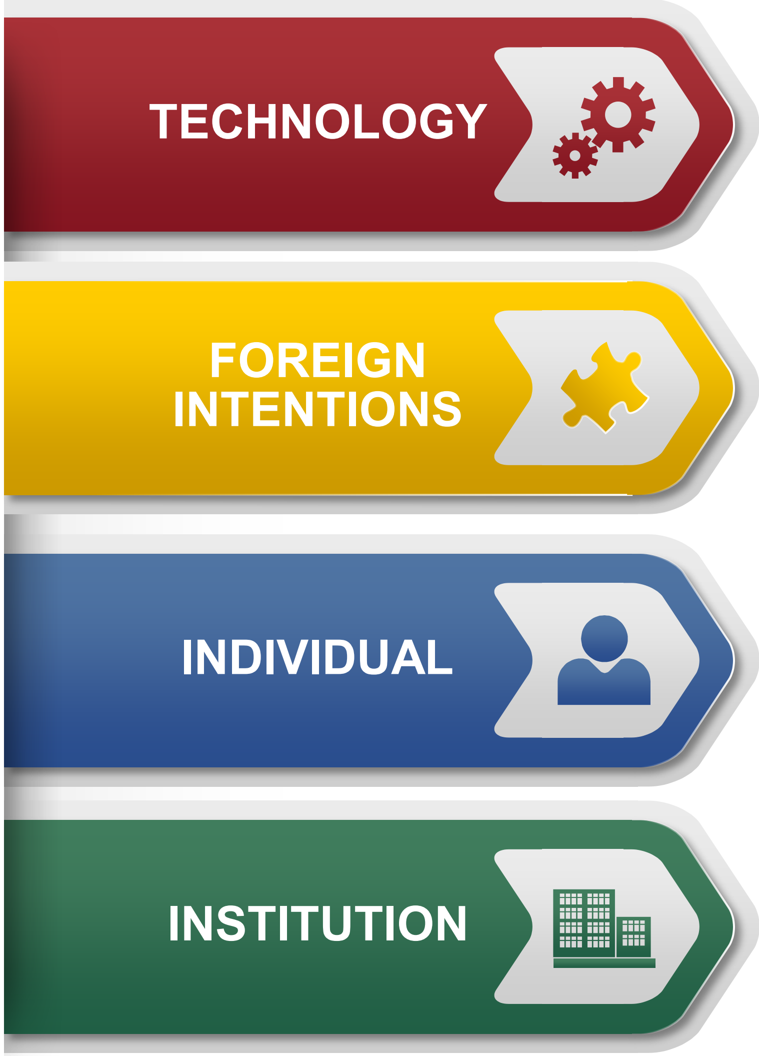
1. *Introduction, Updates, and Responsible Points of Contact (POCs)*
2. *Technology Element Identification and Risk Assessment*
3. *Identified Threats and Vulnerabilities*
4. *Countermeasures and Risk Mitigation Plan*
5. *Response, Recovery, and Support*

Page **1** of **16**

The S&T Protection Plan Template:

- Is a tailorable document for research risk identification and mitigation
- Facilitates discussions between S&T managers, technology subject matter experts, security managers, counterintelligence personnel, and intelligence analysts regarding threat scenarios and appropriate countermeasures
- Is iterative, supporting the continuous identification and documentation of risk factors and countermeasures over a program's lifecycle
- Is informed by the processes and best practices outlined in the S&T Protection Guide

Detailed Risk Assessment



- Developed by an interagency working group (security, export control, grants, and contracts subject matter experts)
- Provides guidance to determine the risk of awarding to, or collaborating with, entities that appear to present greater risk after analysis of risk thresholds
- Utilizes a series of questions and associated risk metrics to assign a value to each of the four quadrants of the risk methodology
- Identifies data and analysis sources to inform the risk assessment process
- Provides DoD Components with a tailorable series of risk definitions that can be applied to grants, contracts, etc.

Distribution Statement A: Approved for public release. DOPSR case #21-S-1241 applies. Distribution is unlimited.

S&T Protection Education

Complete

Defense Acquisition University (DAU) Training

Incorporated changes throughout STM 101 – Introduction to DoD Science & Technology Management. Changes reflect the requirements and best practices outlined in DoDI 5000.83 and related guidance.

DoD Community Outreach

Developed "Security Fundamentals for S&T Professionals" desk reference – Presents a summary of recent developments in research security policy while outlining security resources and best practices.

In Progress

General Research Security

- Best Practices
- Resource Guides
- Integrating research security in additional DoD coursework, national and international forums, etc.

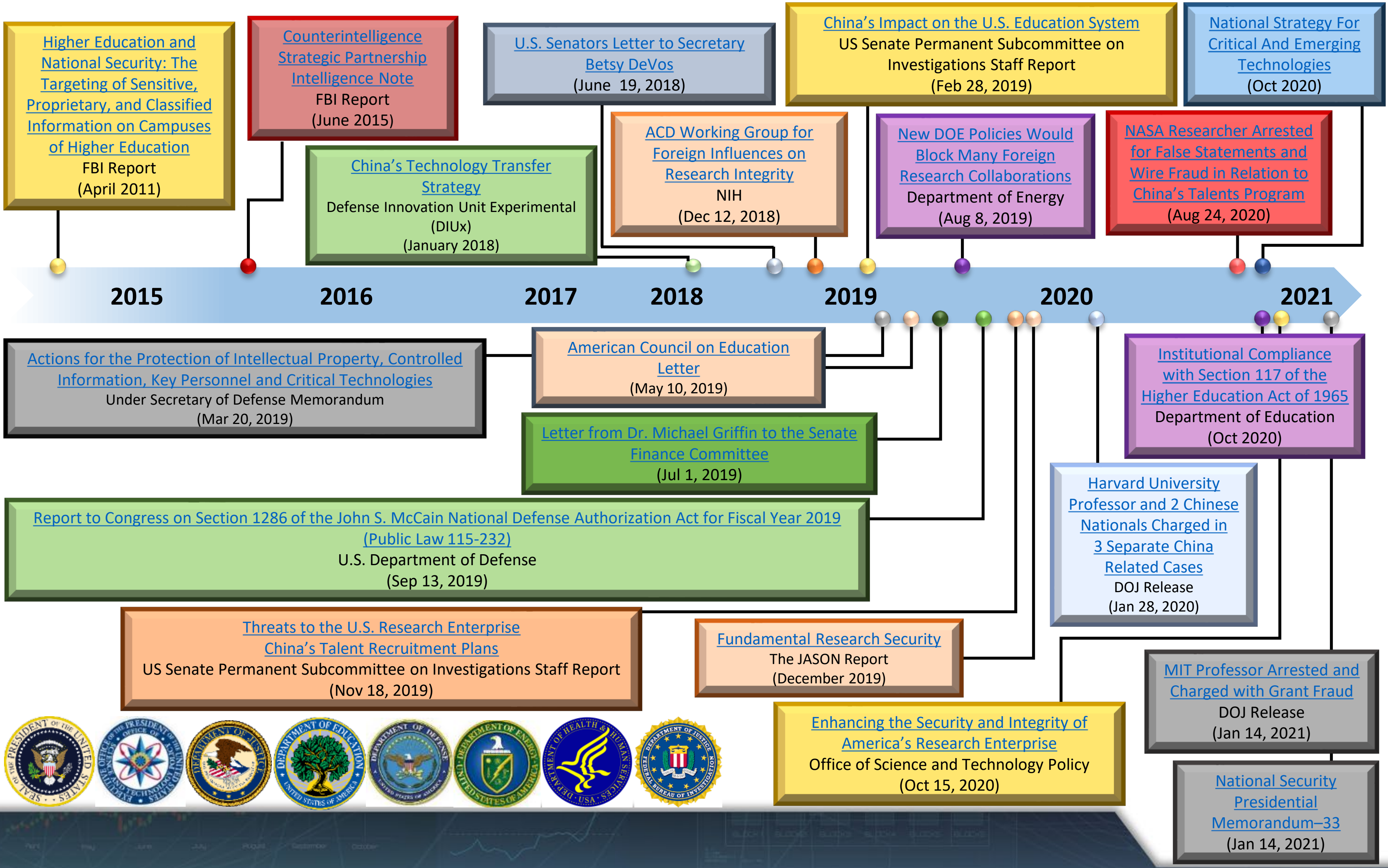
S&T Protection Guide & Template

- "How-To" Guide designed to support DoD components in developing tailored S&T Protection Plans

Risk Analysis Training

- Detailed Risk Methodology
- Identifying risk factors and drafting risk questions to support holistic program protection

U.S. Government Articles, Reports, Letters of Concern to Academia (2011-2021)



Higher Education and National Security: The Targeting of Sensitive, Proprietary, and Classified Information on Campuses of Higher Education
FBI Report
(April 2011)

Counterintelligence Strategic Partnership Intelligence Note
FBI Report
(June 2015)

China's Technology Transfer Strategy
Defense Innovation Unit Experimental (DIUx)
(January 2018)

U.S. Senators Letter to Secretary Betsy DeVos
(June 19, 2018)

ACD Working Group for Foreign Influences on Research Integrity
NIH
(Dec 12, 2018)

China's Impact on the U.S. Education System
US Senate Permanent Subcommittee on Investigations Staff Report
(Feb 28, 2019)

New DOE Policies Would Block Many Foreign Research Collaborations
Department of Energy
(Aug 8, 2019)

NASA Researcher Arrested for False Statements and Wire Fraud in Relation to China's Talents Program
(Aug 24, 2020)

National Strategy For Critical And Emerging Technologies
(Oct 2020)

Actions for the Protection of Intellectual Property, Controlled Information, Key Personnel and Critical Technologies
Under Secretary of Defense Memorandum
(Mar 20, 2019)

American Council on Education Letter
(May 10, 2019)

Letter from Dr. Michael Griffin to the Senate Finance Committee
(Jul 1, 2019)

Report to Congress on Section 1286 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115-232)
U.S. Department of Defense
(Sep 13, 2019)

Threats to the U.S. Research Enterprise China's Talent Recruitment Plans
US Senate Permanent Subcommittee on Investigations Staff Report
(Nov 18, 2019)

Fundamental Research Security
The JASON Report
(December 2019)

Harvard University Professor and 2 Chinese Nationals Charged in 3 Separate China Related Cases
DOJ Release
(Jan 28, 2020)

Enhancing the Security and Integrity of America's Research Enterprise
Office of Science and Technology Policy
(Oct 15, 2020)

Institutional Compliance with Section 117 of the Higher Education Act of 1965
Department of Education
(Oct 2020)

MIT Professor Arrested and Charged with Grant Fraud
DOJ Release
(Jan 14, 2021)

National Security Presidential Memorandum–33
(Jan 14, 2021)

Distribution Statement A: Approved for public release. DOPSR case #21-S-1241 applies. Distribution is unlimited.

Takeaways

- Continue to update and iterate TAPPs with OUSD(R&E) Principal Directors and S&T Communities of Interest
- Engaging with DoD Components to integrate Technology Area Protection Plans into ongoing processes and activities
- Crafting implementation protection policy and align with requirements, acquisition and security policies
- Developing education, training and tools to enable the DoD enterprise
- Engagements for additional horizontal protection including:
  - Small Business Innovation Research
  - International
  - National security innovation base, industrial policy
- Collaborating with organizations across the Federal Government on research security

Comprehensive approach to create and maintain technology advantage

Distribution Statement A: Approved for public release. DOPSR case #21-S-1241 applies. Distribution is unlimited.

Contacts

- Robert Irie, Deputy Director, STP&E
  - robert.e.irie.civ@mail.mil

- Brian Hughes, Director JAPEC, MTA
  - brian.d.hughes3.civ@mail.mil

- Kristopher Gardner, Director S&T Protection, MTA
  - kristopher.e.gardner2.civ@mail.mil

Questions

DoD's Research Security and S&T Protection Efforts to Counter Foreign Influence

PRESENTED BY:

Mr. Kristopher Gardner

Director, S&T Protection, STP&E

Office of the Under Secretary of Defense for Research and Engineering

MODERATED BY:

Steve Redifer

2021-05-13

Homeland Defense & Security Information Analysis Center

HDIAC is sponsored by the Defense Technical Information Center (DTIC). Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Defense Technical Information Center. DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited.

info@hdiac.org
https://www.hdiac.org