

CLEARED  
For Open Publication  
Aug 23, 2023

4  
Department of Defense  
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

# BALANCING OPENNESS AND SECURITY

ACROSS THE DOD ACADEMIC RESEARCH ENTERPRISE

July 2023



DEFENSE SCIENCE BOARD

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.



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 Balancing  
Openness and Security across the DoD Academic Research Enterprise

I am pleased to forward the final report of the DSB Task Force on Balancing Openness and Security Across the DoD Academic Research Enterprise, chaired by Dr. Shirley Ann Jackson. While the issue of balancing openness with security within the DoD academic research enterprise has been an ongoing challenge, the DoD needs a consistent approach in tackling this problem.

As this report makes clear, the two-part threat of being outrun by strategic competitors in the fields of advanced technology along with the counterintelligence threat is real and growing. Adopting more proactive policies will deter aggression by reducing adversary ability to target U.S. institutions and technologies, as well as create an environment for the U.S. to take the lead once again in some critical areas of research.

The recommendations included in this report provide actionable concepts for creating ways to better communicate threat information, protect sensitive technologies, attract talent, and provide for new alternatives for academia to engage in national security science and technology.

I fully endorse the findings and recommendations detailed in this report and urge the Department to quickly implement. Doing so will ensure that the DoD is consistent in its approach and provide the momentum for other government entities to follow.

A handwritten signature in black ink that reads "Eric D. Evans". The signature is written in a cursive, flowing style.

Dr. Eric Evans  
Chair, DSB

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 Balancing Openness and Security Across the DoD Academic Research Enterprise

Attached is the final report of the Defense Science Board Task Force on Balancing Openness and Security Across the DoD Academic Research Enterprise (ARE). The Task Force was asked to consider the most effective ways to address the threat posed by foreign adversaries to the DoD ARE while maintaining the openness required to ensure U.S. academic institutions access the best and the brightest in basic and applied scientific research.

After assembling experts in this field – including academics, law enforcement, and counterintelligence experts – the study reviewed the threat landscape, current U.S. policy and authorities, and the state of DoD involvement in developing and protecting critical technologies. The Task Force assessed and developed key findings and concluded that it is possible to provide additional protection quickly and consistently for the DoD ARE while also maintaining an open and collaborative research environment. The Task Force determined that an adaptable and scalable framework that is consistently reviewed to meet future threats will be necessary for long-term success.

The Task Force urges the Department to review and implement the study's proposals to mitigate the current shortcomings within the DoD ARE. Our strategic competitors are committed to advancement in science and technology and will stop at nothing to obtain the desired results. The recommendations this Task Force provides offer ways to get ahead of the threat while ensuring an open-collaborative research environment where science can thrive.

A handwritten signature in cursive script, reading "Shirley Ann Jackson", is positioned above the typed name.

Dr. Shirley Ann Jackson  
Task Force Chair

THIS PAGE LEFT INTENTIONALLY BLANK

# DSB Final Report on Balancing Openness and Security Across the DoD Academic Research Enterprise

## Table of Contents

<b>Executive Summary</b> .....	<b>1</b>
<b>Context and Understanding the Problem</b> .....	<b>5</b>
<b>The Special Case of China</b> .....	<b>5</b>
China's Requirement for Support of its Law Enforcement and Intelligence Organizations as a Condition of Citizenship .....	7
Illustrative Chinese Technology Collection in the ARE .....	8
<b>The Internal and External Threat</b> .....	<b>9</b>
<b>Task Force Approach</b> .....	<b>9</b>
USD(R&E) Terms of Reference .....	9
Study Framework and Assessment .....	10
Five Overarching Categories of Findings and Recommendations .....	10
<b>Findings and Recommendations</b> .....	<b>11</b>
Threat Awareness .....	11
Findings – Competitive Threats (Being Outrun) .....	11
Findings – Intelligence and Counterintelligence Threats (What We Need to Protect) .....	11
Recommendations .....	12
Understanding/Protecting Sensitive Information .....	12
Findings .....	12
Recommendations .....	13
New Alternatives for Academia Engagement in National Security S&T .....	13
Findings .....	13
Recommendations .....	13
Policies, Guidance, and Authorities .....	15
Findings .....	15
Recommendations .....	15
S&T Talent Attraction, Management, and Oversight .....	16
Findings .....	16
Recommendations .....	16
<b>Appendix A: Task Force Terms of Reference</b> .....	<b>A-1</b>
<b>Appendix B: Task Force Membership</b> .....	<b>B-1</b>
<b>Appendix C: Vignettes</b> .....	<b>C-1</b>
Quantum Information Science (QIS) .....	C-1
Radiation-Hardened Microelectronics .....	C-2
<b>Appendix D: Briefings Received</b> .....	<b>D-1</b>
<b>Appendix E: Acronym List</b> .....	<b>E-1</b>

THIS PAGE LEFT INTENTIONALLY BLANK



# DSB Final Report on Balancing Openness and Security Across the DoD Academic Research Enterprise

---

## Executive Summary

The U.S. science and technology (S&T) ecosystem is the world's largest and most diverse. It is a magnet for scientists, engineers, students, faculty, entrepreneurs, technologically driven businesses, and foreign governments around the world, seeking to emulate its success.

The commercial value of information derived from academic basic and applied research is well understood and allows nations acquiring it to bypass a significant part of the research and development (R&D) process. The substantial rewards of being first-to-market, and the high cost of scientific discovery and technological innovation and maturation, can be powerful incentives for theft. The theft of technology from the academic research enterprise (ARE), including from nations allied to the United States, is an ongoing challenge.

The risk to classified research should not be underestimated as well. The DoD revealed statistics that “nearly a quarter of all foreign efforts to obtain sensitive or classified information in 2014 had been routed through academic institutions.”<sup>1</sup> Shaping the analysis of this study were the plans and activities of countries of concern—China, and like-minded countries such as Russia, Iran, and others.

Much of the information at risk of diversion is not usually classified, but is rather unclassified intellectual property (IP) emerging from applied R&D. Moreover, valuable information may be acquired that is incidental to the research agenda of students and faculty in the ARE, commercial enterprises, or collaborative R&D.

Some of these interactions are not inherently dangerous and are consistent with open research cultures (conferences, lectures, collaborations, etc.) that have led to life-changing advances in the life sciences, information technologies, and manufacturing, among many others. However, obtaining non-public sensitive information can confer commercial, or in some cases, military strategic advantage, and is of particular concern. This is where we find ourselves today—balancing an open research culture against the need to protect sensitive or emerging technologies from those who would do us harm.

This report delineates the results of the work of the Defense Science Board (DSB) Task Force on Balancing Openness and Security Across the DoD Academic Research Enterprise. The terms of reference (ToR), signed on September 20, 2022, by Under Secretary of Defense for Research and Engineering, Heidi Shyu, identified a problem that has become acute and is the focus of this report.

---

<sup>1</sup> Ana Swanson, Keith Bradsher, “White House Considers Restricting Chinese Researchers Over Espionage Fears,” The New York Times, April 30, 2018, <https://www.nytimes.com/2018/04/30/us/politics/trump-china-researchers-espionage.html>

As such, the work of the Task Force was predicated on answering the following questions established in the ToR. The overview responses found in this section provide context and enhancement to the Task Force's findings and recommendations, which begin on page 11.

**How should the DoD best develop research collaborations within the academic research community that yield mutual benefits for all involved?** The Task Force recommendations in response to this question focused on enhancing, strengthening, and expanding what is already working to promote research collaboration such as University Affiliated Research Centers (UARCs), networks of UARCs in critical technology areas, and regional centers of research. The Task Force determined that a call to action is required to address the growing challenge and recommended a "new" National Defense Education Act (NDEA), with financial support and internships for domestic students. Finally, the Task Force found that cybersecurity underpins any actions and programs and believes that the academic research community must do more in its information security approaches to better plan and prepare for the next threat around the corner.

**How should the DoD best implement transparency guidance to assess potential conflicts of interest?** One of the main Task Force findings was the need to improve communication between the United States Government (USG) and academic institutions on local threat awareness. The Task Force framed its recommendations in the areas of required disclosure, with regular updates and monitoring by means of associated digital persistent identifiers (PIDs). In the area of compliance and oversight, additional training modules are needed, with required training once per year for all academic research officials, students, and newly on-boarded individuals.

Generally, smaller universities do not have the resources to be fully aware of and fully connected to insider and outside threats. Therefore, the Task Force recommends that regional infrastructure be established to support such institutions whose researchers are doing important work, but who do not have the built-in expertise of larger institutions. Resource officers or other designated university or regional designees should have the requisite security clearance to receive regular briefings on the threat environment, insider threats, etc. Best practices on threat awareness programs from R1<sup>2</sup> universities and industry should be proliferated by the Government to regional centers and academia.

**How should the Federal and DoD review of a researcher's financial and non-financial ties be done fairly and consistently?** The Task Force heard testimony on challenges posed by a disclosure process which often yields unreliable results. The Task Force recommends that current best practices can be enhanced through an expanded Conflict of Interest (CoI) and Conflict of Commitment (CoC) approach, drawing on export control, International Traffic in Arms Regulations (ITAR) requirements, and business and university IP protection approaches. Scrutiny of requirements for agencies and associated clarification of these requirements should also occur.

---

<sup>2</sup> R1 designations are based on factors related to research and development, including the number of doctoral degrees available, the amount the institution spends on research, the number of research staff in science and engineering fields, and the level of research activity. Specifically, an institution must award at least 20 research/scholarship doctoral degrees in the update year; spend at least \$5 million in total research (as reported through the National Science Foundation Higher Education Research and Development Survey (HERD)).

**How should the DoD determine the areas of research that deserve careful restrictions on openness to protect national security?** The Task Force examined a risk matrix<sup>3</sup> model developed by the Defense Advanced Research Projects Agency (DARPA), which includes triggers defined for key technologies. The Office of the Under Secretary of Defense for Research and Engineering (OUSD (R&E)) subsequently developed a decision risk matrix to be used by DoD components making fundamental research project proposal award decisions.<sup>4</sup> Also, lessons can be learned and applied, as needed, from the Health Insurance Portability and Accountability Act (HIPAA) process, especially for IP protection to implement data protection.

**How should the DoD best keep the academic community up to date on foreign activity that may be damaging to national interests?** Regular briefings from the intelligence and counterintelligence communities on the threat environment are imperative for balancing between openness and protection of information within our academic institutions. The key to bridging communication gaps between the academic and protection communities is imparting threat awareness to academic institutions via the establishment of a designated university or regional official with a clearance sponsored by the DoD. Having the appropriate security clearance would allow for the intelligence and counterintelligence communities to communicate relevant threats and counterintelligence briefings to the ARE. Additionally, the Task Force recommends the USG develop and circulate “no-go” entity lists to the academic research enterprise.<sup>5</sup>

**How should the DoD continue an ongoing review of the openness and security balance across its academic research portfolio?** Continuous dialogue is key in strengthening, clarifying, incorporating, and promulgating disclosure guidance from the White House Office of Science and Technology (OSTP) as it relates to the DoD-funded ARE. The USG should work with university associations or designated officials to develop an insider threat approach to risk management within the ARE, as well as advocate for the use of a risk matrix.

For the DSB sponsor, the Under Secretary of Defense for Research and Engineering (USD(R&E)), the Task Force recommendations can be considered in three overarching categories:

- Those recommendations that USD(R&E) should take the **lead** within DoD. These recommendations are fully within the USD(R&E) purview and can be acted upon unilaterally and moved out on with urgency.
- Those recommendations that USD(R&E) should **champion** within DoD. These recommendations fall within the USD(R&E) scope, but share responsibility with other DoD organizations, requiring partnership for success.

---

<sup>3</sup> Defense Advanced Research Projects Agency (DARPA), <https://www.darpa.mil/work-with-us/for-universities>.

<sup>4</sup> “Department of Defense Strengthening Efforts to Counter Unwanted Foreign Influence on DOD-Funded Research at Institutions of Higher Education,” U.S. Department of Defense, June 30, 2023, <https://www.Defense.Gov/News/Releases/Release/Article/3445601/Department-of-Defense-Strengthening-Efforts-to-Counter-Unwanted-Foreign-Influen/>.

<sup>5</sup> A “no-go” entity list would include those people, organizations, and programs specific to the ARE that DoD-sponsored research entities should refrain from partnering with.

- Those recommendations that USD(R&E) has an ***advocacy role*** with other stakeholders. These recommendations do not fall purely within DoD purview as the lead department, but USD(R&E) maintains a stake in and plays a key advocacy role.

---

## Context and Understanding the Problem

Because the U.S. science and technology (S&T) ecosystem is a magnet for scientists, engineers, students, faculty, entrepreneurs, technologically driven businesses, and foreign governments around the world, the opportunity for unauthorized or illicit technology acquisition has broadened. According to the Federal Bureau of Investigation, “The annual cost to the U.S. economy of counterfeit goods, pirated software, and theft of trade secrets is between \$225 billion and \$600 billion.”<sup>6</sup> Specifically, the theft of technology from the academic research enterprise (ARE), including from nations allied to the United States, remains an ongoing challenge and scopes this Task Force study.

This problem is not a unique U.S. issue, having been cited by numerous countries facing similar challenges. In 2021, Mike Burgess, the Australian Security and Intelligence Organisation director-general said that up to nine countries’ intelligence services are trying to steal or cultivate sensitive research and technology from Australian universities and scientists.<sup>7</sup> In the United Kingdom, the government formed the “Research Collaboration Advice Team,” which will offer confidential security advice to researchers before entering international collaborations to protect research assets from “hostile actors.”<sup>8</sup>

---

## The Special Case of China

The problem of espionage and IP theft is NOT unique to Chinese students, but the scale of the problem is uniquely a Chinese student population problem where the PRC is driving the activities. In comparing the number of international students studying in the United States, the largest university student population of any country comes from China (290,086), compared to Russia with 4,802, Iran with 9,295, India with 199,182, and North Korea with four. Furthermore, in the Netherlands, the Dutch Intelligence Service found IP theft by Chinese students in Dutch universities to be so extensive that a law will be proposed in their parliament to reduce the presence of Chinese students. In July 2022, Ken McCallum, Director General of the UK’s Security Service (MI5), said that MI5 had “more than doubled” its effort against Chinese activity to prevent the theft of sensitive academic research.

The PRC seeks foreign technology wherever it can be acquired. The institutional base for acquiring foreign technology is broad, including collaboration with individual researchers, as well as business, academic, governmental, and research organizations. China is adept at taking advantage of how

---

<sup>6</sup> “Executive Summary - China: The Risk to Corporate America,” FBI, October 4, 2019, <https://www.fbi.gov/file-repository/china-exec-summary-risk-to-corporate-america-2019.pdf/view>.

<sup>7</sup> Andrew Tillett and Julie Hare, “Australian Research at Risk from Multiple Countries, Spy Boss Warns,” Australian Financial Review, March 11, 2021, <https://www.afr.com/politics/federal/australian-research-at-risk-from-multiple-countries-spy-boss-warns-20210311-p579pu>.

<sup>8</sup> Kelly, Éanna, “UK Announces New Unit to Deal with Risk of Foreign Espionage and Theft of IP from Universities.” Science Business, May 26, 2021, <https://sciencebusiness.net/technology-strategy-board/news/uk-announces-new-unit-deal-risk-foreign-espionage-and-theft-ip>.

scientific and technical research is conducted in the United States, where academic institutions and personnel often participate in broad research networks.

In October 2022, Chinese President Xi Jinping directed a change in China's policy on S&T development that emphasizes self-reliance rather than foreign investment and international collaboration.<sup>9</sup> Ironically, China's turn toward S&T developmental self-sufficiency is likely to intensify their efforts to acquire foreign technology by leveraging the international S&T ecosystem wherever and whenever possible.<sup>10</sup> Although the policy change was not formally published by China's State Council (Cabinet) until February 2023, it was widely anticipated in the United States, Europe, and Japan, which led to an increase in narrowly focused export controls on enabling technologies for some of China's key industries, especially in microelectronics.<sup>11</sup>

Following President Xi's directive, China has institutionalized its approach to evade U.S. sanctions and circumvent restrictions on advanced technology.<sup>12</sup> From the perspective of the Task Force, the PRC's efforts to acquire advanced technology from both indigenous development and foreign sources will target the following segments:

- **Technologies where China has a leading position:** electric vehicles (EVs), photovoltaic products, mobile telecommunications, and power grid equipment.
- **Critical areas for development:** large passenger jets, industrial tools and machines, advanced medical and agricultural equipment, defense industry, 5G, advanced microchip development, data center and other IT infrastructure.
- **Emerging technologies:** next-generation communications, new energy, new materials, biotechnology, green technology, and data sciences-related technologies including big data, blockchain, and artificial intelligence.

China's tactics, techniques, and procedures (TTPs) for acquiring foreign technology have been practiced for more than two decades. The acquisition of classified technology is largely in the domain

---

<sup>9</sup> Frank Tan, "Xi Jinping says China must quicken pace of tech self-reliance to prevent being 'strangled by foreign countries'," South China Morning Post, February 2, 2023, [https://www.scmp.com/economy/china-economy/article/3208882/xi-jinping-says-china-must-quicken-pace-tech-self-reliance-prevent-being-strangled-foreign-countries?module=lead\\_hero\\_story&pgtype=homepage](https://www.scmp.com/economy/china-economy/article/3208882/xi-jinping-says-china-must-quicken-pace-tech-self-reliance-prevent-being-strangled-foreign-countries?module=lead_hero_story&pgtype=homepage).

<sup>10</sup> Gordon Corera, "China: MI5 and FBI warn of 'immense' threat," BBC News, July 7, 2022, <https://www.bbc.com/news/world-asia-china-62064506>; Aiken Gump, "Russia, China, Semiconductors and Reimagining National Security: US Export Controls 2022 Year in Review," January 18, 2023, <https://www.akingump.com/en/news-insights/russia-china-semiconductors-and-reimagining-national-security-us-export-controls-2022-year-in-review.html>.

<sup>11</sup> State Council Information Office, "Xi stresses basic research for self-reliance in science and technology," February 22, 2023, [http://english.scio.gov.cn/topnews/2023-02/22/content\\_85121945.htm](http://english.scio.gov.cn/topnews/2023-02/22/content_85121945.htm).

<sup>12</sup> The article was summarized in a Bloomberg article, "China Eyes Thwarting US Chip Curbs," February 21, 2023, [https://www.bloomberg.com/news/articles/2023-02-20/top-chinese-scientists-sketch-out-plans-to-thwart-us-chip-curbs?cmpid=BBD022523\\_NEF&utm\\_medium=email&utm\\_source=newsletter&utm\\_term=230225&utm\\_campaign=nef&leadSource=verify%20wall](https://www.bloomberg.com/news/articles/2023-02-20/top-chinese-scientists-sketch-out-plans-to-thwart-us-chip-curbs?cmpid=BBD022523_NEF&utm_medium=email&utm_source=newsletter&utm_term=230225&utm_campaign=nef&leadSource=verify%20wall). The original Academy of Sciences article is "Scientific Observation/Strengthen the basic capacity building of semiconductors and light up the "lighthouse" of semiconductor self-reliance and self-improvement development," February 16, 2023. "Scientific Observation: Proceedings of the Chinese Academy of Sciences," <https://mp.weixin.qq.com/s/m-WzjLux4HODtYyYKra22w>.

of the Ministry of State Security (MSS) and related People's Liberation Army (PLA) intelligence organizations (including cyber operations). However, Chinese law facilitates the tasking of Chinese citizens by its law enforcement and intelligence services for the acquisition of unclassified technology that may be proprietary or contain trade secrets.

China has sought to leverage its national patent system as a means of exploiting the foreign technology it acquires. China's foreign technology acquisition practice has been to process the technology it acquires through its university system, particularly the PLA-led university system, and obtain Chinese patents. It produces relatively few triadic patents (typically a technology patented in the United States, Europe, and Japan) meant to protect IP on a world-wide basis. U.S. triadic patents, the 'gold standard' of IP, are more than five times the number of Chinese triadic patents. Chinese patents tend to be 'tweaks' of existing IP.

Huawei is the "poster child" for this practice, allowing Huawei to become one of the top patent holders in 5G technology (its patent portfolio includes more than 100,000 patents).<sup>13</sup> Huawei is increasingly seeking to capitalize on revenue from its patent portfolio, and much of that portfolio may have been developed by other, Western organizations. For example, Huawei has sued Verizon for patent infringement, where those patents are believed to have been stolen from Verizon.<sup>14</sup>

### China's Requirement for Support of its Law Enforcement and Intelligence Organizations as a Condition of Citizenship

Following the 19<sup>th</sup> Communist Party of China (CPC) Congress, a law to impose a statutory requirement on all Chinese citizens to respond to requests for assistance by its law enforcement and intelligence services was put into place. The impact of the law has made it possible to institutionalize the process of acquiring technology, legally or illegally from foreign sources, including the United States.

The tasking for all Chinese citizens and organizations in China's S&T ecosystem makes it possible to align foreign technology acquisition with national S&T priorities. The increased bilateral tension between the United States and China, including in trade and scientific collaboration, has produced a significant change in China's acquisition priorities in support of its aspiration for autarky in technology development. China is aggressive in its determination to take the lead in all technology areas. Thus, the focus of its foreign technology collection, including by Chinese personnel able to access the U.S. university and research system, seems likely to intensify.

---

<sup>13</sup> Arjun Kharpal, "Huawei Licenses 5G Patents to Rival as U.S. Sanctions Force the Chinese Giant to Seek New Revenue," CNBC, December 12, 2022, <https://www.cnbc.com/2022/12/09/huawei-licenses-5g-patents-to-rival-as-us-sanctions-bite.html#:~:text=Huawei%20has%20a%20massive%20portfolio.artificial%20intelligence%20and%20autonomous%20cars>.

<sup>14</sup> Igor Bonifacic, "Huawei will use its 5G patents to make money off of other companies," Endgadget, March 16, 2021, <https://www.engadget.com/huawei-5g-patent-licensing-184450343.html> and Kiran Stacey, "US Accuses Huawei of Stealing Technology from Six Companies," Financial Times, February 13, 2020, <https://www.ft.com/content/3174481a-4e8b-11ea-95a0-43d18ec715f5>.



## Illustrative Chinese Technology Collection in the ARE

The following are different practices and methods the PRC uses to gain access to sensitive information within the U.S. ARE. The Task Force realizes other countries may use these practices as well.

1. Tasking of individual Chinese students to collect non-public data relating to their research activities.
2. Sponsorship of Chinese students to participate in academic research and industry conferences to establish informal links with other researchers in fields of interest to China.
3. Creating *ad hoc* lecture and research opportunities in China for leading U.S. academic researchers.
4. Creation of visiting “advisory” or “senior mentor” roles in China for U.S. academic researchers.<sup>15</sup>
5. Establishment of “consulting” opportunities for U.S. academics with Chinese academic, scientific, and industrial research organizations.
6. Establishment of sustained research relationships between Chinese graduate students and U.S. academics when the graduate student studies are completed and returns to China.
7. S&T research collaboration with Chinese entities that result in forced transfer of IP.
8. Establishment of (usually concealed) commercial relationships between Chinese students in the United States and Chinese establishments to acquire foreign technology.<sup>16</sup>
9. Sponsorship of U.S. academic research programs in U.S. universities willing to accept a substantial Chinese student cohort.
10. Leveraging interactions between U.S. technology-based firms and Chinese graduate students to facilitate access to the IP of U.S. firms.<sup>17</sup>
11. Exploiting cyber vulnerabilities within the U.S. ARE, especially in research activities.<sup>18</sup>

---

<sup>15</sup> In a celebrated case, the Chairman of Harvard’s Chemistry Department was convicted of concealing his relationship with China and tax evasion. Department of Justice, “Harvard University Professor Convicted of Making False Statements and Tax Offenses,” December 21, 2021, <https://www.justice.gov/opa/pr/harvard-university-professor-convicted-making-false-statements-and-tax-offenses>.

<sup>16</sup> There has been extensive reporting on China’s technology acquisition from U.S. commercial entities. Sean O’Conner, “How Chinese Companies Facilitate Technology Transfer from the United States,” May 6, 2019, The US-China Economic and Security Review Commission, <https://www.uscc.gov/sites/default/files/Research/How%20Chinese%20Companies%20Facilitate%20Tech%20Transfer%20from%20the%20US.pdf>.

<sup>17</sup> Zachary Cohen and Alex Marquardt, “US Intelligence Warns China Is Using Student Spies to Steal Secrets | CNN Politics,” CNN, February 2, 2019, <https://www.cnn.com/2019/02/01/politics/us-intelligence-chinese-student-espionage/index.html>.

<sup>18</sup> “The China Threat,” FBI, July 10, 2020, <https://www.fbi.gov/investigate/counterintelligence/the-china-threat> and Lindsay McKenzie, “Report: Top Universities in U.S. Targeted by Chinese Hackers,” Inside Higher Ed | Higher



---

## The Internal and External Threat

While the United States faces external threats from hostile actors, it also is confronted with the internal challenge of being competitively outrun. For example, the United States was once the uncontested leader in science and engineering. However, in 2020 the National Science Board and the National Science Foundation released *The State of U.S. Science and Engineering 2020 Report* and concluded that the U.S. has fallen behind in many technology areas.<sup>19</sup> More recently, the Australian Strategic Policy Institute released its report concluding that China is outpacing the United States in 37 out of 44 critical technology research areas.<sup>20</sup>

Therefore, the Task Force study reflects and addresses two fundamental threats that are real and increasingly imminent. There are genuine competitive threats rooted in the existential threat of being outrun in discovery, innovation, and translation. In addition, there are genuine intelligence and counterintelligence threats rooted in inappropriate access to, and exploitation of, sensitive S&T information. Having open science remains vital to innovation and ideas, so a proper balance when implementing solutions to these challenges must be struck.

---

## Task Force Approach

### USD(R&E) Terms of Reference

Throughout the Task Force's deliberations, the questions asked in the *Balancing Openness and Security Across the DoD Academic Research Enterprise* (ARE) Terms of Reference (ToR) were used to inform the Task Force findings and develop the final recommendations.

- How should the DoD best develop research collaborations within the academic research community that yield mutual benefits for all involved?
- How should the DoD best implement transparency guidance to assess potential conflicts of interest?
- How should the USG and DoD review of a researcher's financial and non-financial ties be done fairly and consistently?
- How should the DoD determine the areas of research that deserve careful restrictions on openness to protect national security?
- How should the DoD best keep the academic community up to date on foreign activity that may be damaging to national interests?

---

Education News, Events and Jobs, <https://www.insidehighered.com/news/2019/03/06/report-top-universities-us-targeted-chinese-hackers>.

<sup>19</sup> Beethika Khan, Carol Robbins, and Abigail Okrent, "Science & Engineering Indicators," NSF, <https://www.ncses.nsf.gov/pubs/nsb20201/preface>.

<sup>20</sup> Jamie Gaida et al., "The Global Race for Future Power," ASPI's Critical Technology Tracker - Amazon Web Services, [https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2023-03/ASPIs%20Critical%20Technology%20Tracker\\_0.pdf?VersionId=ndm5v4DRMfpLvu.x69Bi\\_VUdMVLp07jw](https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2023-03/ASPIs%20Critical%20Technology%20Tracker_0.pdf?VersionId=ndm5v4DRMfpLvu.x69Bi_VUdMVLp07jw).

- How should the DoD continue an ongoing review of the openness and security balance across its academic research portfolio?

## Study Framework and Assessment

The Task Force developed a framework for assessing the questions in the study ToR that addressed the perceived threat, how both the USG (and DoD specifically) and the academic institutions have responded to the perceived threats, the security risks associated with key technologies, and the evaluation of new policies or implementation actions that might be useful to address current challenges.

The Task Force first sought to understand the overall threat and risk within the ARE and received a wide range of briefings from law enforcement and counterintelligence entities, university export control and research offices, as well as from DoD laboratories. The Task Force then identified the USG's response to these challenges – both current and historic – by looking at relevant policy and guidance across agencies and institutions. The Task Force assessed the success of the USG response and concluded that the overall approach is not consistent, as different entities and agencies have implemented their own guidance. Additionally, the Task Force found that the emerging Controlled Unclassified Information (CUI) policy and application add to the complexity and confusion.

Then, the Task Force spoke with various university representatives to understand the university response to the problem and reviewed university internal policies and implementation, best practices, current vehicles for handling CUI, talent management, etc. The Task Force found that Most R1 universities have extensive policies, procedures, and training relevant to export controls associated with the academic research enterprise. For example, within the Texas A&M system and at its individual campuses, training and other policies regarding technology transfer are detailed and extensive.

Per the study ToR, the Task Force evaluated the importance of, and risks associated with the 14 critical technologies, delineated by the USD(R&E), at universities and research institutions, as well as the DoD's dependency upon the ARE to support them. The Task Force included vignettes on two critical technologies, quantum science and radiation-hardened microelectronics, which are found in Appendix C.

Once the fact-finding was complete, the Task Force identified current policy gaps and specifically pinpointed the need for clear guidance on the full implementation of *National Security Presidential Memorandum 33* (NSPM-33), as well as CUI clarity and regulatory restraint.

## Five Overarching Categories of Findings and Recommendations

Stemming from Task Force meetings, deliberations, and briefings received from October 2022 through April 2023, the Task Force organized the study assessment, findings, and recommendations into five overarching categories: Threat Awareness; Understanding/Protecting Sensitive Information; New Alternatives for Academia Engagement in National Security S&T; Policies, Guidance, and Authorities; and S&T Talent Attraction, Management, and Oversight.

The Task Force assessment identified improvements needed in the academic research ecosystem right now. And, while some proactive and important activities and programs within the USG and

academic institutions are underway, the seriousness of the problem calls for additional measures. The Task Force's recommendations include what the DoD needs to do, what the ARE should be required to do, and how collaboration among all the stakeholders should be enhanced and expanded.

---

## Findings and Recommendations

### Threat Awareness

#### FINDINGS – COMPETITIVE THREATS (BEING OUTFRONTED)

- While China is not the only country seeking advanced technology and intellectual property from the United States (via legal and illegal means), the PRC's efforts are the most prominent and prolific. **China is outpacing** the U.S. in global competition for key emerging technologies, leading in 37 out of 44 critical and emerging technologies (e.g., electric batteries, hypersonics). Western democracies risk losing the global competition for research output and technological innovation.
- Strategic competitors (China and Russia) are partnering more strongly in key scientific and technology areas, as recommitted in the China-Russia March 2023 joint statement. Moreover, institutions in the European Union and other international institutions are more reluctant to cooperate with U.S. universities and scholars because of the increasing security overlay.
- It is becoming demonstrably more difficult for international scholars to participate in U.S.-sponsored collaborative research; more difficult for U.S. scholars to participate in international activities or to collaborate with foreign nationals in the United States or abroad.
  - If, due to restraints on international collaboration, the United States deprives itself of interaction with key global centers of advancement, its technological progress slows. This, in itself, is a threat to U.S. national security. Open collaboration has been the basis of our scientific prowess.

#### FINDINGS – INTELLIGENCE AND COUNTERINTELLIGENCE THREATS (WHAT WE NEED TO PROTECT)

- University administrators overseeing research are often unaware of, or not trained in, intelligence and security information relevant to making risk-informed mitigations on threats to university research. Often such awareness arises only after investigations are underway.
- Most faculty researchers are unaware of the real threats permeating academic research.<sup>21</sup>
- With respect to insider threats, government agencies and university entities (including the vice presidents for research and related offices) are not always on the same page with respect to investigations of faculty and other researchers.

---

<sup>21</sup> For example, U.S. academic scientists and engineers receive periodic messages/emails of invitation to participate in various foreign government talent recruitment programs and other activities, some of which may be of consequence to U.S. national security.

## RECOMMENDATIONS

- Any DoD entity sponsoring research in academic institutions should develop tailored and current threat training module(s) and require their use by academic researchers accepting DoD funding. The purpose is to heighten understanding of the details of the threat environment in which they operate. This training should not be for classified researchers only, but anyone working in S&T receiving DoD funding with no set dollar amount. This should be consistent, not redundant, with NSPM-33 requirements to NSF.
  - The training should reference deemed export requirements, as well as emphasizing the best practices from the DoD counterintelligence insider threat programs.
- USD(R&E) with USD(I&S) should ensure that academic institutions receiving DoD funding, regardless of amount, have access to research security experts. This could be done by establishing a research security expert position (with requisite DoD-sponsored security clearance at TS/SCI eligibility level) at the university itself, or as part of regional security clusters or centers. The role of these experts would be to liaise with the intelligence community and keep apprised of real-time threats, trends, and forecasts relevant to research. These research security expert(s) would also be responsible for ensuring, within the confines of permitted classification, that information is disseminated to those university personnel who most need to know.
  - USD(R&E) should disseminate among universities that receive DoD funding, the fundamental criteria embedded in the DoD risk matrix,<sup>22</sup> with respect to conflict of interest and conflict of commitment, thereby assisting researchers in understanding undue foreign influence in key technologies critical to DoD.

## Understanding/Protecting Sensitive Information

### FINDINGS

- There is inconsistency across the university research enterprise in approaches to foreign affiliation reporting and disclosure requirements.
- A complication to research security is the lack of clarity with respect to Controlled Unclassified Information (CUI) – in definition, in consistent and comprehensive promulgation of guidance for application, and its application itself, not only in DoD but across the U.S. Government (USG).
- Ambiguity in defining CUI has led to its over-application in certain disciplines, and in certain circumstances, across the USG, which has impacted the academic research enterprise in understanding and adhering to CUI protection requirements (e.g., NIST standards, to include cybersecurity).

---

<sup>22</sup> While this Task Force examined the DARPA risk matrix to develop its findings and recommendations, the OUSD(R&E) subsequently issued the USD(R&E) Memorandum, “Policy for Risk-Based Security Reviews of Fundamental Research”, June 8, 2023, <https://media.defense.gov/2023/Jun/29/2003251160/-1/-1/1/COUNTERING-UNWANTED-INFLUENCE-IN-DEPARTMENT-FUNDED-RESEARCH-AT-INSTITUTIONS-OF-HIGHER-EDUCATION.PDF>.

## RECOMMENDATIONS

- USD(R&E) should work with university associations to create better coherence across universities' approaches to disclosure and protection of sensitive information.
  - Standards and best practices should be codified and shared consistent with the NIST SP 800-171 and 172 series and NDAA 2023 requirements.
  - Best practices should be updated on an ongoing basis and re-disseminated.
- USD(R&E) should require academic research entities receiving DoD funding to strengthen cyber protection with respect to CUI and other sensitive information.
- USD(R&E) should require academic research entities receiving DoD funding to establish a process whereby disclosures are reviewed and updated often, and technology is used for tracking (e.g., digital persistent identifiers, as suggested by the White House Office of Science and Technology Policy (OSTP)).
- USD(R&E), in coordination with USD(P) and USD(I&S), should curate any sensitive entity lists of foreign enterprises (e.g., “Seven Sons of National Defence” in China), which should be shared with universities to improve understanding and oversight of foreign nationals and international entities.
- USD(R&E), through the OSTP Subcommittee on Research Security, should continue to promulgate better guidance to the academic S&T community with respect to the identification and risk assessment of CUI, including the use and refinement of the recently issued DoD risk matrix.

## New Alternatives for Academia Engagement in National Security S&T

### FINDINGS

- The United States is lagging in publications and patents filed in certain key technology areas compared with China (e.g., energy, environment, materials).
- There is insufficient number and breadth of U.S. academic institutions participating in national security S&T.
- A binary decision (i.e., whether DoD-sponsored R&D is open or classified) is disadvantageous for the engagement in national security S&T for universities without requisite infrastructure for classified research, or university policy against such research, in lieu of a spectrum for university-based research which includes collaboration alternatives and cost-sharing approaches to classification requirements.
- There is concern within the academic research community about maintaining free and open research, consistent with the fundamental research exclusion in NSDD-189 and the USD(AT&L) Ashton Carter memorandum on fundamental research (May 24, 2010).

### RECOMMENDATIONS

- Secretary of Defense should direct the creation of Regional Centers of Research (RCRs), to enable participation from a broader range of academic institutions and researchers who may

have the desire/ability to conduct both open and classified research, but not the requisite infrastructure or needed clearances. Requisite facility and personnel security clearances would be available. Such centers would also serve to impart knowledge and awareness of real-time risks to research security. There are three alternatives proposed:

- Requirement for existing DoD laboratories (e.g., AFRL, ONR, ARL, NRL) to provide shared infrastructure to university researchers and their home institutions to perform unclassified and classified research. Each DoD laboratory would sponsor personnel security clearances, as required.
- Expansion of existing DoD laboratories (e.g., AFRL, ONR, ARL, NRL) to establish localized regional centers focused on the critical science and technology areas, linked to their missions.
- Creation of new joint university-federal R&D centers that support unclassified and classified research on emerging foundational challenges in critical technologies for DoD missions. These would span from fundamental to applied research.
- Principal Deputy R&E, Deputy CTO for S&T/OUSD(R&E), and ASD (Industrial Base Policy)/OUSD(A&S), should expand/establish research hubs and forums to bring together small businesses, defense industrial base companies, and universities, that are centers of excellence in S&T undergirding national security, to share ideas and collaborate on critical national security S&T.
  - These would also serve as training centers on security threats and classification requirements.
- USD(R&E), in coordination with the Services, should organize and coordinate CUI-level briefings (e.g., webinars) across the technical mission areas. These briefings would be open to any researcher in the academic enterprise and the subjects would focus on challenges in S&T. The purpose would be to promote and foster greater engagement of academic researchers in national security S&T.
  - USD(R&E) should create a Security Fellows Program to immerse academic researchers in national security S&T challenges. The purpose of the program would be to engage more U.S. citizens in work on national security S&T priorities. The program would have the following characteristics:<sup>23</sup>
    - appointments for a two-year period;
    - monthly meetings;
    - requisite DoD-sponsored security clearances;

---

<sup>23</sup> The Task Force recognizes that similar, ongoing programs (e.g., Defense Science Study Group, Vannevar Bush Faculty Fellowship, and the Minerva Research Initiative) provide great value to researchers and to the DoD. The Task Force recommendation would distinctly focus on technologies critical to the DoD and be open to eligible students as well.

- nominations by academic institutions.

## Policies, Guidance, and Authorities

### FINDINGS

- The complexities in NSPM-33, issued on January 14, 2021, pertaining to Government-Supported Research and Development National Security Policy, show that there is a significant need for clear guidance on full implementation of NSPM-33.
  - This is a quandary for even the exemplar universities who currently allow ITAR and export-controlled research to be pursued on their campuses.
- A key complication in this guidance on research security is the CUI distinction.
  - The lack of clarity in guidance from USG/DoD on CUI (identification and handling) contributes to confusion and uncertainty among academic researchers.
  - Often the “next level” knowledge of national security issues and sensitive information (including CUI) does not reside among academic researchers.

### RECOMMENDATIONS

- USD(R&E) guidance booklet (“DOs and DON’Ts”) of CUI and the DoD risk matrix should be widely promulgated and routinely updated to universities and academic research institutions.
- USD(R&E) should clarify how the fundamental research exclusion is linked, or not linked, to CUI requirements.
- USD(R&E) should ensure timely dissemination of the National Archives CUI Registry to the academic research enterprise. The Registry should be reissued promptly whenever it is updated.
- USD(R&E) and DoD component heads should ensure that training on CUI is available to (and required for) all faculty and researchers working in DoD-funded research, not only in classified research. This training should include clarity in identifying, handling, and implementation of CUI. DoD representatives should visit and conduct training on specific technologies of particular concern. This should be accomplished as an integral part of the normal training process.
- USD(R&E) and Principal Directors in Service Research leadership should create/ensure, using existing mechanisms, an intra-agency group tasked with ensuring consistency in the application of CUI definition across the DoD research enterprise. This should be established as soon as practical.



## S&T Talent Attraction, Management, and Oversight

### FINDINGS

- The United States is facing a decline in overall talent required to significantly advance critical technologies necessary for national security, due to two factors:
  - There has been a significant decline in the participation of U.S. citizens, at the advanced-degree level, in S&T research linked to national security.
  - There is a growing scrutiny of foreign national participation in S&T research, leading to heightened concern about potential discrimination against non-citizens, and a resultant diminution of foreign nationals engaged in advanced S&T research in the United States.
- There is a lack of coordination and continuity in DoD research funding, resulting in significant talent gaps in critical technology areas, and the need in some cases to re-learn what was previously well known.
- There is a lack of timely and effective immigration processes that limit the ability of the USG to recruit and retain additional highly talented individuals.
- There is no specific Startup Visa program focused on foreign nationals who look to start businesses based on S&T research conducted as part of their advanced degree programs in the United States.

### RECOMMENDATIONS

- USD(R&E) with other DoD stakeholders should develop enhanced (depth and breadth) outreach efforts on U.S. university campuses that incentivize S&T undergraduates to pursue advanced degrees in research relevant to the DoD and national security.
- Basic Research officials in DoD should enhance and stably fund existing programs for students to carry out collaborative research in DoD laboratories, including in non-restrictive areas for international students. Students could be paired with designated Government-Owned, Contractor-Operated (GOCO) entities during part of their research program.
- USD(P), with USD(R&E) and other key USG stakeholders, should advocate creating a Startup Visa program to incentivize and allow those foreign nationals who have received advanced S&T degrees in the United States to remain and start businesses based on their advanced degree work.<sup>24</sup>
- USD(P) and USD(R&E), with support from other key USG stakeholders, should establish partnerships with U.S.-friendly nations. These partnerships should include institutions within Latin America, India, and Africa – targeted toward those countries having a concentration of high-quality universities. Ultimately, qualified academic institutions on each continent should be included.

---

<sup>24</sup> Specifically, this would be beneficial to the DoD by retaining critical talent working on key technologies. And, while there is an U.S. entrepreneur visa, its purpose is to promote entrepreneurship and job creation in the United States, but is not focused on retaining the foreign talent resident in academia.



- USD(P) in coordination with USD(R&E) and USD(A&S) should mandate that all DoD-funded research have a requirement for the use of the E-Verify system by awardees, as currently required of contractors under the Federal Acquisition Regulation (FAR) clause.
- USD(P) with support from other key DoD stakeholders should work with the interagency to develop a consistent and coordinated entry/re-entry process of foreign scholars that is underpinned by appropriate risk assessment using the E-Verify system.
- USD(R&E) working with academic institutions should develop/issue a “guidebook” for onboarding international science scholars (students and postdocs) and promulgate to international scholars and faculty advisors. The purpose would be to serve as a “rule of the road” for understanding the expectations and culture of U.S. scientific research.
- Secretary of Defense should propose in the next budget cycle the reenactment of the *National Defense Education Act* to support education and training of U.S. citizens in national security S&T and to support the expansion and continuity of research funding in critical S&T areas:
  - Multi-year continuity of research funding in critical areas
  - Undergraduate scholarships
  - Graduate fellowships
  - Undergraduate and graduate internship and research opportunities at DoD laboratories and other S&T facilities

THIS PAGE LEFT INTENTIONALLY BLANK

## Appendix A: Task Force Terms of Reference



UNDER SECRETARY OF DEFENSE  
3030 DEFENSE PENTAGON  
WASHINGTON, DC 20301-3000

CLEARÉD  
For Open Publication  
4  
Oct 04, 2022  
Department of Defense  
OFFICE OF PUBLICATION AND SECURITY REVIEW

20 SEP 2022

MEMORANDUM FOR CHAIR, DEFENSE SCIENCE BOARD

SUBJECT: Terms of Reference – Defense Science Board Task Force on Balancing Openness and Security Across the DoD Academic Research Enterprise

The U.S. academic research enterprise is central to our nation's leadership in fundamental scientific advances, technology development, and engineering excellence for a wide range of global needs. A core attribute of a strong research enterprise is the significant flow of ideas through academic partnerships, open publication, and technology transition across the academic community, including through research across national boundaries. The U.S. has been highly successful in advancing new frontiers of knowledge through open research collaboration with academic partners around the world.

For some technology areas, the U.S. may also need to protect certain aspects of its research investment to ensure that potential adversaries do not use particular research results or technologies to damage or degrade U.S. economic strengths, national security, or human rights. For some areas, the U.S. may need to develop a balance between academic openness and national security to enable the advancement of knowledge without damaging our national interests. This balance may require some limited restrictions on access and information sharing, as well as improved conflict-of-interest transparency for current and future research. The right balance must be evaluated and implemented very carefully and consistently to ensure that the constraints do not do more harm than good.

I am establishing the Task Force on Balancing Openness and Security Across the Department of Defense (DoD) Academic Research Enterprise ("the Task Force") as a subcommittee of the Defense Science Board (DSB). The DSB, working through the Task Force, should review the Under Secretary of Defense for Research and Engineering (USD(R&E)) fourteen Critical Technology Areas<sup>1</sup> and provide a report with recommendations regarding a decision framework that achieves the right balance of openness and security for each area. The Task Force should consider:

- How should the DoD best develop research collaborations within the academic research community that yield mutual benefits for all involved?

<sup>1</sup> In February 2022 the published the *USD(R&E) Technology Vision for an Era of Competition*, recognizing fourteen Critical Technology Areas vital to the United States' national security: Biotechnology, Quantum Science, Future Generation Wireless Technology (FutureG), Advanced Materials, Trusted AI and Autonomy, Integrated Network Systems-of-Systems, Microelectronics, Space Technology, Renewable Energy Generation and Storage, Advanced Computing and Software, Human-Machine Interfaces, Directed Energy, Hypersonics, and Integrated Sensing and Cyber.

- How should the DoD best implement transparency guidance to assess potential conflicts of interest?
- How should federal government and DoD review of a researcher's financial and non-financial ties be done fairly and consistently?
- How should the DoD determine the areas of research that deserve careful restrictions on openness to protect national security?
- How should the DoD best keep the academic community up to date on foreign activity that may be damaging to national interests?
- How should the DoD continue an ongoing review of the openness and security balance across its academic research portfolio?

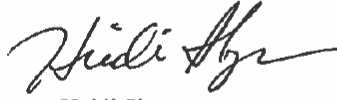
The Task Force findings, observations, and recommendations will be presented to the full DSB for its thorough, open discussion and deliberation at a properly noticed and public meeting, subject to the Government in the Sunshine Act exemptions. The DSB will provide its findings and recommendations to the USD(R&E) as the Sponsor of the DSB. The nominal start date of the study period will be within 30 days of the initial appointment of Task Force members. In no event will the duration of the Task Force exceed 12 months from the start date.

In support of this Terms of Reference (ToR) and the work conducted in response to it, the DSB and the Task Force have my full support to meet with Department leaders. The DSB staff, on behalf of the DSB and the Task Force, may request the Office of the Secretary of Defense and DoD Component Heads to timely furnish any requested information, assistance, or access to personnel to the DSB or the Task Force. All requests shall be consistent with applicable laws, applicable security classifications, DoD Instruction 5105.04, "Department of Defense Federal Advisory Committee Management Program," and this ToR. As special government employee members of a DoD federal advisory committee, the DSB and the Task Force members will not be given any access to DoD networks, to include DoD email systems.

Once material is provided to the DSB and the Task Force, it becomes a permanent part of the DSB's records. All data/information provided is subject to public inspection unless the originating Component office properly marks the data/information with the appropriate classification and Freedom of Information Act exemption categories before the data/information is released to the DSB and the Task Force. The DSB has physical storage capability and electronic storage and communications capability on both unclassified and classified networks to support receipt of material up to the TS/SCI level.

The DSB and the Task Force will operate in conformity with and pursuant to the DSB's charter, the Federal Advisory Committee Act (5 United States Code (U.S.C.), Appendix), the Government in the Sunshine Act (5 U.S.C. § 552b), and other applicable federal statutes, regulations, and policy. Individual DSB and Task Force members and the Task Force as a whole do not have the authority to make decisions or provide recommendations on behalf of the DSB nor report directly to any Federal representative. The members of the Task Force and the DSB are

subject to certain Federal ethics laws, including 18 U.S.C. § 208, governing conflicts of interest, and the Standards of Ethical Conduct regulations in 5 Code of Federal Regulations, Part 2635.



Heidi Shyu

---

## Appendix B: Task Force Membership

### Task Force Chair

Dr. Shirley Ann Jackson

### Task Force Members

Dr. Jennifer Bernhard  
Honorable Michael Bayer  
Mr. Tomás Díaz de la Rubia  
Dr. Robert Grossman  
Dr. Ayanna Howard  
Dr. Evelyn Hu  
Dr. Ashanti Johnson  
Dr. Ann Karagozian  
Honorable Judith Miller  
Dr. DJ Patil  
Dr. Sanjay Raman  
Dr. David Relman  
Dr. William Schneider

### DSB Secretariat

Ms. Elizabeth Kowalski, Designated Federal Officer  
Mr. Kevin Doxey, DSB Executive Director

### Study Support

Ms. Brenda Poole (SAIC)  
Ms. Kathryn Hein (SAIC)

---

## Appendix C: Vignettes

The Task Force examined several of the 14 critical technologies,<sup>25</sup> two of which we highlight in this section—Quantum Information Science and Radiation-Hardened Microelectronics.

### Quantum Information Science (QIS)

Quantum-based technologies undergird vibrant economies that can provide agile, sophisticated solutions for broad societal challenges. Such technologies include the Global Positioning System (GPS) for navigation, Magnetic Resonance Imaging (MRI) for medical imaging, semiconductors for computer chips, and lasers for telecommunications. Recent progress in the control of materials and information at the atomic scale has led to what some term a “Second Quantum Revolution,” allowing far more powerful approaches to computing, communications, and sensing. There has been a global recognition and promise of this Quantum Information Science (QIS). For example, within the United States, the *National Quantum Initiative Act* provides for a coordinated federal program to accelerate quantum research and development for the economic and national security of the United States.

Quantum Information Science and Engineering (QISE) occupies a distinctive, perhaps singular point in technology development. While companies such as IBM, Microsoft, and Google are moving forward with the development of QIS systems, there remain profound challenges in the coherent performance of small, still nascent systems, with much development required in the architecture, control, correction, engineering, and manufacture of such systems. Thus, QIS falls within all “bins”: (1) Seed Areas of Emerging Opportunity, (2) Effective Adoption Areas, and (3) Defense-Specific Areas. This characterization provides nuances in the balance between research openness and national security risks.

As an example, quantum networks, comprised of numerous building-block nodes, are being developed to distribute quantum states (information) between geographically remote clients.

The commercial possibilities of such quantum networks are profound: these could serve as the basis of secure communications or quantum computing clusters. There are obvious DoD needs for such capabilities, beyond commercial opportunities.

However, although there are proof of concept experiments being carried out both globally (e.g., in the Netherlands) and in the United States, even the physical platforms of such networks are not fully determined. That is, the choice of qubit, its ultimate coherent behavior, the methods and quality of control, the best, and the lowest-loss means of transmission from node-to-node, are all very much the subject of basic research.

Thus, the national security risks do not only encompass the loss of the following critical technologies to competitors:

---

<sup>25</sup> “Critical Technology Areas,” DoD Research & Engineering, OUSD(R&E), [cto.mil/usdre-strat-vision-critical-tech-areas/](https://cto.mil/usdre-strat-vision-critical-tech-areas/).

- Loss of technologies for secure communications in overhead satellite surveillance, land, and sea-based surveillance and under conflict situations.
- Loss of technologies for high-speed encryption and decryption.
- Loss of technologies for high-sensitivity quantum sensors for queuing and surveillance.

The risks also pertain to severe restrictions of openness of the academic research sector, the curtailment of global collaborations, and the restriction/reduction of talented young researchers addressing these scientific and technological challenges.<sup>26</sup> In short, there is a risk that these technologies will not be able to make the transition from fundamental scientific understanding to engineered possibility, to practical deployment.

QIS is still a broad technological area and is not fully understood in terms of topical sub-areas and state of development that may be a critical trigger point for full understanding of the balance between openness and security.

### Radiation-Hardened Microelectronics

The “digital revolution” and launching of the “information age” has been driven by advances in microelectronics, quantified by the iconic “Moore’s Law” doubling of the number of transistors on a chip, roughly every two years. The concomitant shrinkage of transistor size has allowed for denser information capabilities at low cost, but the state-of-the-art “(SOTA) node” moving to three nanometers and billions of transistors per chip, requires multi-billion-dollar investments in equipment, design and manufacturing expertise, and fabrication plants, currently the purview of very few global companies (TSMC, Samsung, and Intel).

The DoD has critical needs for updated microelectronics to carry out C5ISR (command, control, computer, communications, cyber intelligence, surveillance and reconnaissance) in its systems, with some key additional requirements for radiation-tolerant or radiation-hardened (rad-hard or RH) microelectronics. Space-based systems face an environment that includes geomagnetically trapped particles, solar energetic particles, and galactic cosmic rays. Strategic radiation hardened (SRH) microelectronics must face man-made radiation (e.g., from nuclear detonations). In particular, requirements include:

- Rad-hard microelectronics for space: satellite surveillance, communications, data-handling.
- Rad-hard microelectronics for offensive and defensive security: sensors for timely warning, agility in guiding and controlling offensive and defensive weapons.
- Microelectronics that can survive nuclear and directed energy environments.

However, today’s microelectronics market is dominated by consumer-demand, rather than defense-demand, and the base of RH and SRH suppliers has been shrinking. This shrinkage compounded by the dramatic consolidation of SOTA microelectronics manufacturing capability comprise a profound

---

<sup>26</sup> We note that there has already been a report disseminated on the *Role of Foreign Talent in Quantum Information Science*.



national security risk. While the CHIPS Act<sup>27</sup> provides funding to augment U.S. research, workforce development, and manufacturing of semiconductors, it does not explicitly address the issue of RD/SRH microelectronics.

A possible solution for long-term design, manufacture, and accessibility to RH/SRH may reside in leveraging capabilities of SOTA (or near-SOTA) foundries, with appropriate understanding of the radiation effects at the device level and appropriate re-design of SOTA chips, as concluded in a recent JASON study (JSR-21-05, *Radiation-Hard Microelectronics*, Jan. 2022). Current studies suggest that the reduced dimensions of SOTA microelectronics may render them more robust to “single event upsets” (SEUs).<sup>28</sup> Those studies have been carried out by university/national laboratory collaborations and are relevant to future considerations of balancing open academic research in the service of national security.

In addition to the national security risks regarding the loss of RH/SRH microelectronics in the applications cited above, securing future capabilities in RH/SRH microelectronics depends on continued workforce development in these aspects of microelectronics design and manufacturing. In addition, such development/education must also focus on the effects of radiation environments on those microelectronic systems. To achieve this, consideration must be given of access to challenges of RH/SRH microelectronic systems in national defense environments.

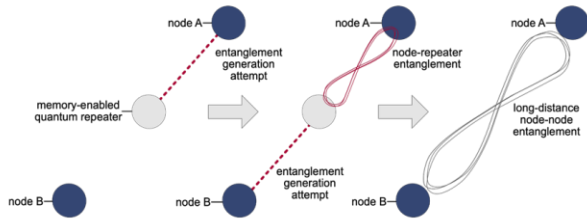
---

<sup>27</sup> “Biden-Harris Administration Launches First Chips for America Funding Opportunity,” U.S. Department of Commerce, February 28, 2023, <https://www.commerce.gov/news/press-releases/2023/02/biden-harris-administration-launches-first-chips-america-funding>.

<sup>28</sup> 1. N. J. Pieper et al., “Single-Event Upsets for Single-Port and Two-Port SRAM Cells at the 5-Nm Finfet Technology,” *IEEE Transactions on Nuclear Science*, 2023, 1–1, <https://doi.org/10.1109/tns.2023.3240979>.

## Vignette #1.

### Quantum Science: An Opportunity



#### OPPORTUNITY: QUANTUM NETWORKS: USED TO DISTRIBUTE QUANTUM STATES BETWEEN REMOTE CLIENTS

#### COMMERCIAL POSSIBILITIES

- Secure communications
- Quantum computing clusters
- Note that new applications will emerge once the characteristics of Quantum Networks begin to be more fully implemented and realized.

#### NATIONAL SECURITY RISKS

- Loss of technologies for secure communications in overhead satellite surveillance, land and sea-based surveillance, and in warfare.
- Loss of technologies for high-speed encryption and decryption.
- Loss of technologies for high-sensitivity quantum sensors for queuing and surveillance.

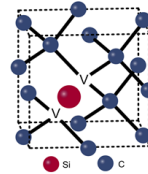
**Balance:** National Security Risks with the tremendous need for Fundamental Research from a Global Community in order to make these technologies feasible.

### Quantum Networks: A Possible Implementation

#### REQUIREMENTS

- Long-lived quantum memory
- Efficient spin-photon interface
- Access to many qubits
- Coherent photons
- Scalable
- High-temperature operation

“Silicon vacancies” in diamond:  
a possible qubit



#### FUNDAMENTAL RESEARCH

- Choice of qubits (e.g. color centers in diamond or silicon)
- Control of qubit formation, coherence, indistinguishability, transport
- Network “backbone”: photonic circuits
- Network architectures and algorithms

Important systems-level implementation depend on the fundamental control & performance of the qubits.

The “advanced materials” needed to realize Quantum Networks

## Vignette #2.

### Radiation-Hardened Microelectronics

#### NATIONAL SECURITY RISKS

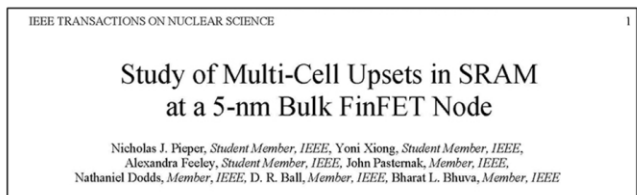
- Need for rad-hard microelectronics for space: satellite surveillance, communications, data-handling.
- Need for rad-hard microelectronics for offensive and defensive security: sensors for timely warning, agility in guiding and controlling offensive and defensive weapons.
- Issues of survivability for microelectronics under critical conditions (nuclear, directed energy environments).
- Issues for the DoD: the continued availability of rad-hard microelectronics with State-of-the-Art (SOA) performance and reasonable cost.
- This area has cross-cutting issues for a host of the other 14 critical technologies.

How and why would open, fundamental, and University-based research play a role here?

### Radiation-Hardened Microelectronics: A Role for Open Research?

#### DEVELOPING A SUSTAINABLE, SOA RAD-HARD MICROELECTRONIC TECHNOLOGY REQUIRES A BROAD INVESTMENT IN FUNDAMENTAL RESEARCH.

- **Fundamental research** on circuit upsets due to alpha particles, 14-MeV neutrons, thermal neutrons, and heavy ions
- Critical innovations in test, evaluation, and understanding of SOA under radiation must be led by academia and National Labs
  - Open Literature Publication
  - Student co-authors
- Innovations in SOA circuit design reside in industry: academia can be a conduit and co-innovator in that area



---

## Appendix D: Briefings Received

### 8 November 2022

Balancing Openness and Security across the DoD Academic Research Enterprise  
*Association of American Universities (AAU)*

Panel Discussion on Academic Research Challenges  
*IBM, Texas A&M, Georgia Institute of Technology, PCAST*

### 14 December 2022

NCITF Perspective  
*National Counterintelligence Task Force (NCITF)*

ICE “Project Shield America”  
*U.S. Immigration and Customs Enforcement (ICE), Department of Homeland Security (DHS)*

OUSD(R&E) Basic Research Perspective, Academic Research Protection Overview  
*Office of the Under Secretary of Defense for Research and Engineering OUSD(R&E)*

Counterintelligence & Security Integration and Threats to Technology  
*Office of the Under Secretary of Defense for Research and Engineering OUSD(R&E)*

### 18 January 2023

DHS Perspective, Office of University Programs Overview  
*Department of Homeland Security (DHS), S&T Directorate*

DCSA Perspective  
*Defense Counterintelligence and Security Agency (DCSA)*

NSF Perspective, Balancing Openness and Security in NSF-funded Research  
*National Science Foundation (NSF)*

Protecting US Biomedical Science from Undue Foreign Interference: NIH Perspective  
*National Institutes of Health (NIH)*

### 14 February 2023

Balancing Openness and Security across the DoD Academic Research Enterprise:  
JHAPL Perspective (*Classified Discussion*)  
*John Hopkins University Applied Physics Laboratory (JHUAPL)*

OSTP Perspective (*Classified Discussion*)  
*White House Office of Science and Technology Policy (OSTP)*

ARLIS Remarks to ARE Task Force (*Classified Discussion*)  
*Applied Research Laboratory for Intelligence and Security (ARLIS)*

LLNL Perspective (*Classified Discussion*)

*Lawrence Livermore National Laboratory (LLNL)*

### 20 March 2023

OUSD(R&E) Perspective  
*HON Heidi Shyu (USD(R&E))*

Texas A&M Office of Research  
*Texas A&M*

State Department Perspective: Visas MANTIS Overview and Student Visa Process and Screening  
*U.S. Department of State*

Naval Research Laboratory Perspective  
*Naval Research Laboratory (NRL)*

Update from OUSD(R&E) Basic Research Directorate  
*Office of the Under Secretary of Defense for Research and Engineering OUSD(R&E)*

### 31 March 2023

Science and Technology (S&T) Program Protection (STPP) Perspective  
*Office of the Under Secretary of Defense for Research and Engineering OUSD(R&E)*

### 4 April 2023

Protecting the Research Enterprise, Texas A&M Perspective – Part 2  
*Texas A&M*

### 13 April 2023

China Threat Brief  
*Army G-2*

Academia and FBI  
*SNIO for China, Federal Bureau of Investigation (FBI)*

DARPA Perspective  
*Defense Advanced Research Projects Agency (DARPA)*

---

## Appendix E: Acronym List

AFRL	Air Force Research Laboratory
ARE	academic research enterprise
ARL	Army Research Laboratory
C5ISR	command, control, computer, communications, cyber intelligence, surveillance and reconnaissance
CI	counterintelligence
CoC	conflicts of commitment
CoI	conflicts of interest
CPC	Communist Party of China
CTO	Chief Technology Officer
CUI	controlled unclassified information
CWHTUST	country with a history of targeting U.S. technologies
DARPA	Defense Advanced Research Projects Agency
DoD	Department of Defense
DSB	Defense Science Board
EO	executive order
EV	electric vehicle
FAR	Federal Acquisition Regulation
GOCO	government-owned, contractor-operated
GPS	global positioning System
HIPAA	Health Insurance Portability and Accountability Act
IC	intelligence community
IP	intellectual property
ITAR	International Traffic in Arms Regulations
MSS	Ministry of State Security
MRI	magnetic resonance imaging
NDAA	National Defense Authorization Act

NDEA	National Defense Education Act
NIST	National Institute of Standards and Technology
NRL	national research laboratory
NSDD	National Security Decision Directive
NSF	National Science Foundation
NSPM-33	National Security Presidential Memorandum-33
ONR	Office of Naval Research
OSTP	White House Office of Science and Technology Policy
PIDs	digital persistent identifiers
PLA	People's Liberation Army
QIS	quantum information science
QISE	quantum information science and engineering
R&D	research and development
RH	radiation-hardened
S&T	science & technology
SOTA	state-of-the-art
SRH	strategic radiation-hardened
ToR	terms of reference
TS/SCI	top secret/ sensitive compartmented information
TTPs	tactics, techniques, and procedures
UARCs	University-Affiliated Research Center Laboratories
USD(A&S)	Under Secretary of Defense for Acquisition and Sustainment
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(I&S)	Under Secretary of Defense for Intelligence and Security
USD(P)	Under Secretary of Defense for Policy
USD(R&E)	Under Secretary of Defense for Research and Engineering
USG	United States Government