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

RESEARCH
AND ENGINEERING

OCT 1 0 2019

Dear Academic Colleagues:

For decades, scientists at universities and research centers, supported by the Department of Defense (DoD), have made ground-breaking scientific discoveries that underpinned dramatic commercial and national security advances, significantly improving the lives of citizens here and abroad. DoD recognizes the contribution of research integrity principles, such as the free exchange of ideas, transparency, and collaboration across research communities as critical to our mutual success. Yet today, the ability to make similar advances is at risk, and research integrity is jeopardized through foreign governments' exploitation that intentionally target U.S. and allied partner research and intellectual capital.

We must find ways to protect research integrity that has contributed to the creation of the finest research institutions in the world and allows us to attract the necessary talent to maintain our economic and national security. The principles of integrity, openness, reciprocity, merit-based competition, and transparency are the foundation of American innovation. The theft of controlled information and unethical diversion of intellectual capital threatens both the American economy and the security of our nation. I request your assistance to preserve the long-standing norms and ethical behaviors that have benefited our research institutions.

The challenge of protecting the integrity of our research enterprise is a national priority. In his September 16, 2019, letter[1] to the research community, Dr. Kelvin Droegemeier, Director of the White House Office of Science and Technology Policy (OSTP), described a new OSTP-led interagency Joint Committee on the Research Environment (JCORE). DoD is an active participant in JCORE, and in its sub-committee on Research Security, which is initially focused on coordinating four lines of Federal effort: coordinating outreach and engagement; disclosure requirements for participation in federally funded research; best practices for academic research institutions; and methods for identification, assessment, and management of risk. This work will help agencies that fund Federal research to develop common standards for identifying and adjudicating conflicts of interest and conflicts of commitment from these disclosures. It will also help agencies that fund Federal research to clarify consequences for failing to make these disclosures.

Even prior to the establishment of JCORE, DoD has taken several steps to address this rising threat and protect open research at U.S. institutions. In October 2018, the Secretary of Defense formed the Protecting Critical Technology Task Force to work across the defense industry and research enterprise toward these goals. On March 20, 2019, to address conflicts of interest and conflicts of commitment, I signed a memorandum[2] requiring that all research and research-related educational activities conducted through DoD research grants, cooperative agreements, Technology Investment Agreements, and other non-procurement transactions require key personnel to disclose

---

[1] https://www.whitehouse.gov/wp-content/uploads/2019/09/OSTP-letter-to-the-US-research-community-september-2019.pdf

[2] Dr. Michael D. Griffin, Under Secretary of Defense for Research and Engineering, Memorandum titled "Actions for the Protection of Intellectual Property, Controlled Information, Key Personnel and Critical Technologies," dated March 20, 2019.

all current and pending projects, time commitments to other projects, and funding sources at the time of application. I expect your support to ensure your faculty meets these new reporting requirements. We will use this information to limit undue influence by countries that desire to exploit DoD research, science and technology, and innovation enterprise through foreign talent programs and other means.

As additional steps, the Department is pursuing a Government-wide approach to ensure appropriate control of our science and technology investments, consistent protection of critical technologies, and elimination of foreign exploitation and influence to counter this threat. No laboratory, university, industry partner, or Government agency can address the full scope of this challenge alone, and solutions to this problem can only result from a dynamic partnership between our public and private sectors. To that end, I request your assistance in identifying and taking action against illegal activities and unethical practices across your research enterprise. I encourage you to partner with DoD Program Officers, the Defense Counterintelligence and Security Agency, the Defense Criminal Investigative Service, the Air Force Office of Special Investigations, the Army Criminal Investigation Division, the Army Counterintelligence Division, the Naval Criminal Investigative Service, and/or the Federal Bureau of Investigation, which all work to support and protect the DoD research enterprise. Together they stand ready to leverage their organizational capabilities and authorities to aid you.

I also seek your help in developing and implementing solutions and best practices and participating in threat awareness and information sharing. I appreciate the many ongoing activities by educational organizations such as the American Council on Education (ACE), the Association of American Universities (AAU), the Association of Public and Land-grant Universities (APLU), and the Academic Security and Counter Exploitation (ASCE) Working Group to address the threats posed by foreign governments exploiting the research community. I encourage you to read and consider implementing the effective policies and practices compiled by the AAU and the APLU in the April 22, 2019, report *Actions Taken by Universities to Address Growing Concerns about Security Threats and Undue Foreign Influence on Campus,*[3] and the addendum to the ACE letter of May 10, 2019,[4] and to support participation in the ASCE[5] Working Group.

Open international collaborations are important to DoD and the Nation, and we must also protect against those who seek to exploit this openness. Let us redouble our efforts to protect research integrity and intellectual capital while seeking a long-term competitive advantage and premier innovation enterprise. Thank you for your leadership on this critical issue.

Please contact Brian Hughes (brian.d.hughes3.civ@mail.mil) or Kristopher Gardner (kristopher.e.gardner2.civ@mail.mil) from the Office of the Under Secretary of Defense for Research and Engineering with any questions on this matter.

Sincerely,

Michael D. Griffin

---

[3] https://www.aplu.org/members/councils/governmental-affairs/cga-miscellaneous-documents/Effective-Sci-Sec-Practices-What-Campuses-are-Doing.pdf

[4] https://www.acenet.edu/Documents/Memo-ACE-membership-foreign-espionage.pdf

[5] https://asce.tamus.edu