Recommendations to OSTP on National Security Presidential Memorandum-33

Emily Weinstein
Center for Security and Emerging Technology

Ainikki Riikonen
Center for a New American Security

November 9th, 2021

Background: The White House Office of Science and Technology Policy is asking the research community for best practices and policy prescriptions for securing certain U.S. government research and development (R&D) efforts. On August 10, 2021, OSTP Director Dr. Eric Lander published a statement, entitled "Clear Rules for Research Security and Researcher Responsibility," in which he laid out the Biden administration's plans to develop clear and effective implementation guidance for National Security Presidential Memorandum-33 (NSPM-33). This document, issued in the final days of the Trump administration, is intended to "strengthen protections of United States Government-supported R&D against foreign government interference and exploitation" while "maintaining an open environment to foster research discoveries and innovation that benefit our nation and the world."

In conjunction with the National Security Council, Cabinet agencies, and other federal agencies, OSTP seeks to address three primary areas of concern: 1) disclosure policy, 2) oversight and enforcement, and 3) research security programs.

Our submission recommends:

- **OSTP should spearhead the creation of harmonized conflict of interest (COI) policies and disclosure requirements across U.S. government agencies that issue basic fundamental research grants.**
- **OSTP should encourage the establishment of an amnesty program for COI reporting during the period of FY2023-2025 to allow universities and research institutions the opportunity to align their institutional policies with anticipated new requirements from the federal government.**
- **OSTP should spearhead a communications and outreach strategy regarding the roles and responsibilities across the research security ecosystem.**

OSTP should spearhead the creation of harmonized conflict of interest (COI) policies and disclosure requirements across U.S. government agencies that issue fundamental research grants.

Relevant parties across the interagency, led by OSTP, should develop standard conflict of interest (COI) policies for all federally funded fundamental research, as defined by the National Security Decision Directive 189 (NSDD-189).[1] Federal agencies that fund research, including the National Science Foundation (NSF), National Institutes of Health (NIH), NASA, the Department of Defense (DOD), and others, currently have different disclosure requirements, which have and will continue to cause undue confusion among researchers and universities.[2]

- As recommended by the 2019 JASON Report, "Fundamental Research Security," the disclosure process should be expanded to include full disclosure of commitments as well as actual or potential conflicts of interest.[3]
- On an annual basis, all recipients of federal research grants will be required to submit new COI and disclosure forms via Grants.gov. This annual submission will count towards all federally funded basic research projects to which an individual is attached.
- Research that is deemed to be sensitive from a national security point of view, as defined under National Security Decision Directive 189 (NSDD-189) and classified under Executive Order 12356, may require additional and/or more stringent disclosure requirements on top of the harmonized COIs.

As part of efforts to harmonize policies, OSTP should also lead in the development of standard definitions associated with research security. OSTP should convene interagency and university stakeholders following the model of the Joint Committee on Research Environments (JCORE).[4] Common definitions should then be communicated across the research security ecosystem, including to law enforcement agencies, as these would bolster understanding of the role that relevant parties play in the process.

- Funding agencies should develop common language to define the relevant parties in a research grant, including clarifying who the "grantee" is, in contrast to the "principal investigator." This should be done in consultation with universities, research institutions, and other relevant parties.
    - For example, a university could be the "grantee," and a specific professor could be the "principal investigator." In any instances of wrongdoing in the grant application process, enforcement agencies can refer first to the university itself as the front line of the enforcement ecosystem and facilitator of reporting processes.

---

[1] "Fundamental research" in this context can be viewed in a similar capacity to DOD's 6.1 basic research, as defined by the DOD RDT&E Budget Activity Codes.
https://www.nsf.gov/news/special_reports/jasonsecurity/JSR-19-2IFundamentalResearchSecurity_12062019FINAL.pdf

[2] https://science.house.gov/imo/media/doc/Wright%20Testimony2.pdf

[3] https://www.nsf.gov/news/special_reports/jasonsecurity/JSR-19-2IFundamentalResearchSecurity_12062019FINAL.pdf

[4] https://trumpwhitehouse.archives.gov/ostp/nstc/

- As outlined in the 2019 JASON Report, the current accepted definition of "research misconduct," based on a reaffirmed 1992 definition, is outdated.[5] Research agencies, both public and private, must update these terms to reflect the current environment.
- Although there have already been several attempts in Congress to define a "malign foreign talent recruitment program" as per the House-passed version of the 2022 NDAA, federal research agencies should decide on and promulgate a country-agnostic definition for "malign foreign talent recruitment programs."[6]

OSTP should encourage the establishment of an amnesty program for COI reporting during the period of FY 2023-2025 to allow universities and research institutions the opportunity to align their institutional policies with anticipated new requirements from the federal government.

OSTP should encourage agencies with enforcement responsibilities, including funding agencies and the FBI, to extend a period of amnesty to grant applicants for new COI disclosures not previously reported. The timeline should extend to the ***first*** *application* submitted after FY2023—the new fiscal year after funding agencies have standardized disclosure policies and processes according to NSPM-33's one-year deadline for implementation. This amnesty program should end after FY2025.

- The speed to which research security policy has changed, as well as the lack of clarity in disclosure requirements, has led to false positives that undermine the efficacy of government research security efforts, and public trust in those efforts. The lack of clarity has also hampered applicants' ability to understand and thereby comply with existing requirements.
- Functionally, a period of amnesty would give time for universities and grantees to acclimate to the new and clarified requirements. It would also strengthen enforcement efforts by reducing barriers to submitting accurate new reporting and paving the way for better information available to investigators and policymakers alike.
- Under this period of amnesty, all those receiving federal research grants, and who have foreign appointments or are part of foreign talent programs, should be required to disclose this information.
- A period of amnesty for researchers could also prove insightful for counterintelligence agencies to learn more about adversary tactics and strategies.
- Backsliding or multiple offenses should be investigated and if appropriate, fairly prosecuted, and those who are found to deliberately break regulations or laws should be penalized accordingly.[7]

[5] https://www.nsf.gov/news/special_reports/jasonsecurity/JSR-19-2IFundamentalResearchSecurity_12062019FINAL.pdf
[6] https://www.congress.gov/bill/117th-congress/house-bill/4350/text
[7] Hannas, William C. and Tatlow, Didi Kirsten, *Beyond Espionage: China's Quest for Foreign Technology* (Routledge, 2021).

OSTP should spearhead a communications and outreach strategy regarding the roles and responsibilities across the research security ecosystem.

As recommended in the House-passed version of the 2022 NDAA, federal research agencies, led by OSTP, should establish a requirement that organizations that win research grants from the agency must complete research security training, and ensure that all relevant individuals employed by the institution or organization are listed on the application and made aware of the training requirement.[8]

- The training guidelines should be developed by the Director of OSTP, acting through the National Science and Technology Council.
- OSTP, in conjunction with the Directors of the NSF and NIH, should find a qualified party to develop online research security training modules that focus on but are not limited to the following subjects:
    - International collaboration and travel, including conferences and field research;
    - Foreign interference;
    - Rules for proper use of funds;
    - Rules for proper disclosure, conflict of commitment, and conflict of interest policies.

OSTP should spearhead the convening and solicit funding of an independent, public-private institution that can inform and support research security efforts throughout the U.S.'s R&D ecosystem.[9] This institution should:

- Work in conjunction with federal agencies that mitigate technology transfer to build dialogue with research organizations' research security programs to socialize awareness of technologies at risk for theft.[10]
- Provide researchers and institutions with context-specific, data-driven threat assessments to allow them to assess risks to research security in any specific situation;
- Track security trends and threats across the U.S. research landscape—regardless of whether or not the threats implicate violations of law—and develop and disseminate defensive best practices;
- Employ staff from the both interagency and relevant public with technical expertise and experience in relevant subjects, such as:
    - Language and area studies knowledge pertaining to "foreign countries of concern" as determined by the Department of State;
    - S&T;
    - Counterintelligence;
    - Open-source data analysis and data visualization.

---

[8] https://www.congress.gov/bill/117th-congress/house-bill/4350/text

[9] https://cset.georgetown.edu/publication/bolstering-u-s-research-security/

[10] https://www.cnas.org/publications/reports/the-american-ai-century-a-blueprint-for-action.
As a model, the Bureau of Industry and Security at the Department of Commerce trains colleges and universities on export control laws, and the State Department's Bureau of Democracy, Human Rights, and Labor can provide guidance for institutions developing technologies that can be misused for authoritarian surveillance and human rights abuses. For more information, see: https://www.bis.doc.gov/index.php/online-training-room, and https://www.state.gov/key-topics-bureau-of-democracy-human-rights-and-labor/due-diligence-guidance/