Defense Advanced Research Projects Agency (DARPA) Fundamental Research Risk-Based Security Review Program (FRRBS)

Summary Q&A: DARPA Fundamental Research Workshop with Vice Provosts of Research, Academic Leaders

Timed with the start of the Fall 2024 academic year, 200 university leaders from 106 institutions gathered virtually and on-site at DARPA for a workshop to discuss the agency's Fundamental Risk-Based Security Review process.

The Fundamental Research Risk-Based Security Review (FRRBS) is an analytical risk review process focused on identifying and mitigating undue foreign influence in Department of Defense science and technology research grants and cooperative agreements by identifying possible conflicts of interest or commitment by academic researchers. DARPA uses a risk-based evaluation matrix to assess potential researchers' undue foreign influence-related conflicts of interest or conflicts of commitment based on information institutions submit as part of their fundamental research grant/cooperative agreement proposals.

DARPA implemented its policy in accordance with the Office of the Under Secretary of Defense for Research and Engineering OUSD(R&E) policy on Risk-Based Security Reviews and Fundamental Research.

Hosted in partnership with the research community, the DARPA workshop aimed to understand impacts to – and policies implemented by – academic institutions to remain in compliance with the program. Further, DARPA sought to create a space for academic leaders to share best practices among their peers to navigate challenges and mitigate risk. The slides presented during the workshop are available on the DARPA website.

Throughout the workshop, university leaders shared the difficulty navigating disparate guidance across federal funders and varying approaches among academic institutions for training of faculty and staff to identify and mitigate risk. The discourse also highlighted the cultural challenge for university researchers who rely on broad academic collaboration.

DARPA is providing this summary with a dual purpose:

- Inform those university leaders and by extension, academic researchers, who were unable to attend the event either in-person or virtually, and
- Share with workshop attendees the common conversations across the various breakout groups.

Complementary to a list of frequently asked questions available on the DARPA website, the following is an edited summary of questions and comments compiled during the workshop main discussion and breakout sessions, organized by topic.

Consistency of Implementation

Q1: Attendees noted inconsistency in how terms such as covered individual are interpreted, what information is required for compliance, and asked: *Are there plans to institute a consistent protocol across Federal agencies and the Department of Defense?*

A1a: *The term "covered individuals" is defined in Section 10638 of the CHIPS and Science Act of 2022 and should be applied consistently throughout the government.*

A1b: *All DoD organizations are now required to utilize the rubric in the USD(R&E) policy for standardization. While use of the OUSD(R&E) matrix in the policy is required, DoD components and agencies have the option to add supplemental criteria to the matrix for evaluation based on their internal requirements. Other DoD agencies may be less "risk tolerant" and may have more stringent criteria than DARPA.*

A1c: Several o*ther USG agencies (e.g. NSF, NIH, IARPA) are working closely with DARPA in establishing their own fundamental research security review programs. While they may mirror a significant portion of the DoD & DARPA policy framework, each agency will have their own unique requirements necessary to establish their policies and procedures.*

Q2: Attendees noted that requests related to mitigation plans may go directly to the principal investigators. Without a consistent process in place, the appropriate university office may not be notified. Are there plans for a formal tracking system?

A2: *Yes, OUSD(R&E) is developing a process to track mitigation strategies so when developed, reciprocity between agencies may be easier to accomplish. OUSD(R&E) is also comparing agency policies to highlight major differences between implementation strategies to try and streamline them and standardize them as much as practical.*

Q3: Can universities/principal investigators report on a quarterly basis rather than as requests come in, as a timed reporting structure would be easier to implement consistently?

A3: *DARPA does not have issue with consolidating reporting requirements/timelines to align with a quarterly basis (or as required). If the initial reporting date does not align with an established reporting period, please let us know and we can adjust reporting times as necessary.*

Covered Individuals

Q4: Can you point to a standard definition of Covered Individual, as they differ among institutions and among the DOD?

A4: DARPA relies on the definition included in Section 10638 of the CHIPS and Science Act of 2022, which defines "covered individual" as "an individual who (A) contributes in a substantive, meaningful way to the scientific development or execution of a research and development project proposed to be carried out with a research and development award from a Federal research agency; and (B) is designated as a covered individual by the Federal research agency concerned."

Q5: If an employee in the lab, but not on a DARPA project, is offered a job in one of the organizations on the prohibited list, how should the principal investigator navigate the situation? What is the reporting requirement?

A5: *It is recommended, although not required, that the principal investigator (PI) contact their DARPA program POC (typically the program manager (PM)) to discuss the issue with the technical office Program Security Officer (PSO) and the DARPA SID-CFIP Lead. The PM, PSO, and CFIP Lead can provide potential or probable issues and outcomes to the PI for discussion points with the employee in question.*

Q6: What is the process when a post doc or other individual originally deemed eligible becomes affiliated with an organization identified as malign? Similar to the question above, what is the correct course of action if they stay with the university or the lab, but are no longer on the DARPA effort?

A6: *NSPM-33, OUSD(R&E) and DARPA policies are specifically applied to "covered individuals" only. Post-docs, grad students, and other research employees are not currently subject the provisions in these policies. However, their participation on DoD funded programs may call into the integrity of that institution and researchers by allowing prohibited participation in a malign organization by an academic/industry organizational employee when this behavior is otherwise expressly prohibited.*

Q7: What happens when a person or entity falsely claims affiliation with an institution? How does the FRRBS process/security team address that when the university has informed the government it is a false narrative, but have no resource in taking down false information on other websites?

A7a: *False claims made by the individual working on a DoD funded program should be addressed through verification and validation of the "claimed" information with the organization claimed against. If verified as "false" and not corrected by the researcher, it can be viewed as "providing a materially false statement or fact" which may subject that researcher to debarment from federal funding.*

A7b: *If an organization is making a false claim about a researcher's affiliation, then that affiliation should be challenged by the individual in question through their academic research security office (or other appropriate office). If the organization is unwilling to correct the information, then it's recommended that the researcher provides an affidavit stating that this is a false claim by the organization and they've taken appropriate steps to remediate this falsehood.*

Definition of Malign Foreign Talent Recruitment Program

Q8: Why is the DARPA definition of Malign Foreign Talent Recruitment Program referenced in the workshop presentation different from that issued by OSTP?

A8: *There is no difference. DARPA and OSTP refer to the definition included in the CHIPS and Science Act of 2022.*

Information Classification

Q9: What is the process for marking documents as controlled unclassified information (CUI) and why does it take so long to recategorize documents incorrectly marked as CUI?

A9: *Marking CUI information within the DoD is done in accordance with DoD Instruction 5200.48, Controlled Unclassified Information (CUI). For DARPA specific programs that contain CUI, a CUI*

Guide (CUIG) is generated by the PSO of the technical office that outlines how to mark and protect the program specific information identified as CUI. Decontrolling CUI / recategorizing incorrectly marked CUI requires a review and evaluation of the incorrectly marked information, comparing it against the CUIG issued, any potential CUI categories the information may fall under (e.g. Export Control Regulations, ITAR/USML, Proprietary Information, Defense Critical Infrastructure, Operational Security, Privacy Information, etc.) and the S&T Protection Plan for the program. Information is reviewed and evaluated by the PSO, Chief of Information Security, Foreign Disclosure Officer, and Public Affairs Office for potential public release.

Training – Universities

Q10: Can the government provide training modules with the core knowledge content, which institutions may adapt based on needs?

A10: *The National Science Foundation provides academic institution and industry training on Research Security. It can be found at: https://new.nsf.gov/research-security/training.*

Training – Small Business

Q11: Attendees noted that universities serving as subs to small business primes find it challenging to navigate issues such as handling of controlled unclassified information. The universities who serve as subs also noted they are generally not allowed/discouraged from contacting the contracting officer to access more information on security protocol. *Has DARPA or another Government agency considered offering a training specific to small businesses on how to navigate FRRBS as they are often primes or subcontractors to universities?*

A11a: *DARPA has provided policy information, a comprehensive FAQ on FRRBS, and the VPR Workshop presentation that are available for public release on our website: https://www.darpa.mil/work-with-us/communities/academia.*

A11b: *DARPA encourages all organizations (prime/sub, academic/ industry) to contact the program's Program Security Representative (PSR) or PSO for security related information. While the primary route of contact for a sub should be through the prime, if specific questions regarding a sub's security posture or issues arises, and the prime is unable to provide adequate information, it is strongly encouraged to contact the DARPA PSO/PSR directly to avoid any potential security related issues. However, please be sure to cc the prime POC for their situational awareness.*

A11c: T*raining resources for CUI and other security related topics can be found through the Defense Counterintelligence and Security Agency's (DCSA) Center for Development of Security Excellence (CDSE). https://securityawareness.usalearning.gov/cui/index.html, https://www.cdse.edu/Training/eLearning/IF141/, and https://www.dodcui.mil/Training/.*