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

RESEARCH
AND ENGINEERING

JUN 0 8 2023

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR ACQUISITION AND SUSTAINMENT
SECRETARY OF THE ARMY
SECRETARY OF THE AIR FORCE
SECRETARY OF THE NAVY
COMMANDER, UNITED STATES SPECIAL OPERATIONS COMMAND
COMMANDER, UNITED STATES CYBER COMMAND
COMMANDER, UNITED STATES STRATEGIC COMMAND
DIRECTOR, MISSILE DEFENSE AGENCY
DIRECTOR, DEFENSE ADVANCED RESEARCH PROJECTS AGENCY
DIRECTOR, DEFENSE THREAT REDUCTION AGENCY

SUBJECT: Policy for Risk-Based Security Reviews of Fundamental Research

References: (a) National Security Presidential Memorandum-33, "United States Government-Supported Research and Development National Security Policy," January 14, 2021
(b) National Science and Technology Council Report, "Guidance for Implementing National Security Presidential Memorandum-33 (NSPM-33) on National Security Strategy for United States Government-Supported Research and Development," January 2022
(c) Department of Defense Memorandum on National Security Presidential Memorandum-33 Implementation, December 14, 2022

Background

This memorandum provides policy for the risk-based security reviews mandated by section 1286 of the National Defense Authorization Act for Fiscal Year 2019 and National Security Presidential Memorandum-33 (NSPM-33), "United States Government-Supported Research and Development National Security Policy," dated January 14, 2021 (reference (a)). The overall intent of this policy is to ensure consistent application of risk-based security reviews for fundamental research project proposals across the Department of Defense (DoD). The Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)) will oversee the review processes developed by the DoD Components.

In the DoD Memorandum on National Security Presidential Memorandum-33 Implementation, dated December 14, 2022 (reference (c)), the Deputy Secretary of Defense, assigned the Under Secretary of Defense for Research and Engineering (USD(R&E)) the responsibility for overseeing DoD's NSPM-33 implementation and directed the USD(R&E) to compile and disseminate a draft Department-level NSPM-33 implementation plan. This memorandum fulfills part of the Department's NSPM-33 implementation plan.

As part of the broader U.S. Government effort to combat undue foreign influence in Federally funded scientific research, DoD Components shall follow the policies contained in this memorandum for risk-based security reviews of fundamental research project proposals to mitigate potential research security risks uncovered during a risk-based security review in compliance with NSPM-33, ensure alignment between the DoD Components, and support the Department's mission.

Research institutions are of vital importance to the Department. The Department's goals in conducting risk-based security reviews of fundamental research project proposals are:

- To ensure the security of DoD-funded fundamental research;
- To ensure that covered individuals fully disclose information that can reveal potential conflicts of interest and conflicts of commitment; and
- To provide clear messaging to those conducting fundamental research on acceptable and encouraged behaviors as well as activities that may lead to challenges in securing DoD research funding.

Many in the academic community were unaware of the research security risks associated with some foreign governments, including through foreign government-sponsored talent recruitment programs, before the Department and other Federal agencies began taking action to inform academia of these threats. On October 10, 2019, the Department, through the USD(R&E), sent a letter to the academic community concerning the risk of foreign influence in academia. As such, DoD policies should not typically view disclosed conduct or actions that were not seen as risky prior to the Department's admonition as indicative of security risks.

The policies outlined in this memorandum will allow the OUSD(R&E) to work with the Office of Science and Technology Policy (OSTP) and the rest of the U.S. Government to ensure that a consistent, all-of-Government risk-based security review process is implemented as required by OSTP's National Science and Technology Council guidance on NSPM-33 implementation.

Policies for Risk-Based Security Reviews

Each DoD Component shall develop a risk-based security review process to identify fundamental research project proposals' research security risk mitigation needs. Risk-based security reviews shall be conducted, at a minimum, on all fundamental research project proposals that are ***selected for award based on technical merit***. DoD Components shall develop risk-based security review processes:

- That employ the Science and Technology (S&T) Protection Guide, dated March 31, 2021 (or updated version), Appendix B, "Fundamental Research Review Template," to verify that the fundamental research project proposal meets the criteria of fundamental research identified in Appendix B;

- That are consistent with the attached "DoD Component Decision Matrix to Inform Fundamental Research Proposal Mitigation Decisions" (decision matrix) to assess fundamental research project proposals' risk mitigation needs. The OUSD(R&E) will maintain the decision matrix at https://basicresearch.defense.gov/Programs/Academic-Research-Security/. DoD Components must verify they are using the most up-to-date version of the decision matrix by referring to the version posted at the aforementioned website;

- That use the disclosures and Standard Form 424 submitted by the proposing institution for all covered individuals listed in fundamental research project proposals selected for award to identify potential research security risks and employ relevant publicly available information, at a minimum, to verify the information submitted in the disclosures and Standard Form 424;

- That conduct an annual review of funded research projects using the Research Performance Progress Report (RPPR);

- In a manner that does not discourage international research collaboration;

- In a manner that balances the goal of minimizing time-to-award with the need to conduct an effective risk-based security review. For the purposes of this balance, the time taken by the responsible contracting officer, grants officer, agreements officer or their representatives to negotiate risk mitigation measures with the proposing institution is not to be considered as part of the time-to-award;

- In a manner that ensures no additional delay to award if the fundamental research project proposal is assessed, using the decision matrix, as not requiring measures to mitigate research security risk. If the initial risk-based security review assesses any risk factor in Table 1 of the decision matrix as potentially requiring mitigation, the fundamental research project proposal will be referred for further review per the processes defined by the DoD Component in its risk-based security review process; and

- That institute policies defining the level of research security risk mitigation determination that is appropriate for the DoD Component to follow its customary process to recommend and make funding decisions and when a decision by Component leadership (or designee) is required.

DoD Components are encouraged and allowed to further analyze risk-based security reviews of already funded fundamental research projects against broader risk factors, determined by the DoD Component, to generate a comprehensive portfolio analysis and empower leadership with enhanced situational awareness.

Policies for Research Security Risk-Based Mitigation Decisions

To the maximum extent practicable, DoD Components shall seek to mitigate any research security risks uncovered through risk-based security reviews. Strategies to mitigate research security risks include, but are not limited to, requiring the proposing institution to:

- Require the covered individual(s) to complete insider risk awareness training;
- Require increased frequency of reporting by the covered individual(s) through the RPPR;
- Replace individuals listed in the fundamental research project proposal who are deemed a research security risk;
- Provide DoD the covered individual's(s') contracts for review and clarify relationships, affiliations, and/or associations considered risky; and
- Require the covered individual(s) to resign from positions deemed problematic by the risk-based security review.

Verification that a covered individual possesses a Top Secret clearance with a U.S. Government department or agency, if applicable, is also an appropriate mitigation strategy. All enacted mitigation strategies must be submitted to and accepted by the awarding office in writing.

Policies for Rejection of a Fundamental Research Project Proposal Based on Research Security Risk

When the decision not to make an award (i.e., rejection of a fundamental research project proposal) is not based on technical merit and is instead based on research security risks that cannot be mitigated, DoD Components shall adhere to the following policies:

- Rejection of a fundamental research project proposal based on a risk-based security review shall only occur when Component leadership (or designee) determines that one or more research security risks are unable to be mitigated and that the risks are unacceptable.
    - Research security risk factors that may not be able to be mitigated are typically those rated as "Mitigation measures required" or prohibited by law in Table 1 of the decision matrix; or
    - Cases where the DoD Component and proposing institution are unable to come to an agreement concerning proposed mitigation strategies.
- Any rejection of a fundamental research project proposal based on a risk-based security review shall be explained in a risk-based security review rejection letter to

the proposing institution. The risk-based security review rejection letter shall provide sufficient information to enable the proposing institution to make an informed response.

- Upon rejecting a fundamental research project proposal based on a risk-based security review, the DoD Component shall send copies of the risk-based security review rejection letter to the OUSD(R&E). The OUSD(R&E) will disseminate the findings disclosed in the risk-based security review rejection letter to other DoD Components, as appropriate.

Policies for Ensuring Consistency of Risk-Based Security Review Process

To ensure the Department's risk-based security review processes are consistent internally and with other Federal agencies, DoD Components shall adhere to the following policies:

- DoD Components must record their risk-based security review process and policies and provide them to the OUSD(R&E).

- In order to verify that risk-based security review processes are appropriately identifying research security risks, DoD Components must conduct periodic spot checks of covered individuals listed on representative samples of fundamental research project proposals the Component selects for award to identify any research security risks that were missed during the initial risk-based security review. Component spot checks should focus on those fundamental research project proposals which have not been previously assessed as potentially needing mitigation and undergone further review.

- This spot check process, including intended frequency and sample size, must be documented in the DoD Components' risk-based review process. To ensure compliance with the policies prescribed in this memo, the OUSD(R&E) may also conduct spot checks of a DoD Component's risk-based security reviews. The OUSD(R&E) will immediately request a revision of the Component's policy if the spot check reveals differences between the Component's risk assessments and the risk factors in the decision matrix.

- DoD Components must provide informal summaries of all risk-based security reviews to the OUSD(R&E), using the schedule outlined in the decision matrix. These informal summaries must include the number of risk-based security reviews conducted, the number of fundamental research project proposals rejected based on risk-based security reviews, and descriptions of the research security risks that led to each proposal's rejection.

- If a proposing institution challenges a DoD Component's rejection of a fundamental research project proposal made on the basis of a risk-based security review, the Component shall refer the challenge to the OUSD(R&E) for mediation. The OUSD(R&E) will review, and potentially change, the findings of the risk-based

security review to ensure it was conducted in a manner consistent with the policies in this memorandum and factors found in the decision matrix.

  - If the OUSD(R&E) review determines that a DoD Component's risk-based security review of a fundamental research project proposal was conducted in a manner inconsistent with, or based on misinterpretation of, the policies in this memorandum or factors in the decision matrix, the OUSD(R&E) may change the Component's risk determination. The fundamental research project proposal will then be returned to the Component for funding decision and implementation of mitigation strategies as appropriate.

- If a DoD Component rejects potential fundamental research project proposals on the basis of risk-based security reviews in a manner that the OUSD(R&E) determines is inconsistent with other DoD Components or Federal agencies, the OUSD(R&E) and the DoD Component will review the Component's risk-based security review process to identify the source of the inconsistencies.

- If a DoD Component's risk-based security review process uncovers a gap in the decision matrix, the OUSD(R&E) will adjust the decision matrix as appropriate.

The OUSD(R&E) will update the decision matrix as necessary to incorporate changes in law and policy, account for lessons learned, and ensure consistency with other Federal agencies. Updates to the decision matrix will be discussed and disseminated through the Defense Basic Research Advisory Group, OUSD(R&E) S&T Protection Working Group, and posted at https://basicresearch.defense.gov/Programs/Academic-Research-Security/. Definitions for key terms related to this policy are also included in the decision matrix.

Heidi Shyu

Attachment(s):
As stated

cc:
Under Secretary of Defense for Policy
Under Secretary of Defense for Intelligence and Security