August
2026

PROTECTING YOUR EXPERTISE

A GUIDE FOR THE DEFENSE RESEARCH COMMUNITY

JOB AID

CDSE Center for Development of Security Excellence

INTRODUCTION

This job aid serves as a counterintelligence guide for members of the defense research community to identify and mitigate any **foreign intelligence entity (FIE)** targeting Department of War (DoW) innovation. Because this community often relies on open collaboration, adversaries exploit this accessibility to siphon research and expertise. This guide empowers professionals to protect their expertise and secure innovation by integrating counterintelligence best practices into common aspects of their interactions.

WHAT IS THE THREAT TO THE INNOVATION ECOSYSTEM?

A primary threat is the exploitation and illicit acquisition of foundational research *before* it becomes classified or export controlled. FIEs and their proxies hide behind legitimate-looking funding and collaborative opportunities to gain access to critical DoW innovation and expertise. This job aid provides a framework to evaluate the risk from both financial sponsorships and non-financial academic engagements.

The **defense research community**, an often-interconnected ecosystem of professionals developing advanced technology for national security, includes:

- **DoW and government research and development (R&D) personnel:** Scientists, engineers, and program managers at DoW labs, innovation hubs, and agencies.
- **Academic partners:** University professors, graduate researchers, and staff at University-Affiliated Research Centers (UARC) or those receiving defense grants.
- **Defense industry innovators:** R&D personnel at cleared defense contractors developing future capabilities.
- **Institutes and advisory bodies:** Subject-matter experts at think tanks, Federally Funded Research and Development Centers (FFRDC), and scientific journals providing peer reviews or strategic analysis.

THE OBJECTIVE: COLLABORATION WITH SECURITY

Open collaboration is essential for innovation, but it must be balanced with counterintelligence to protect national security assets. The objective is to engage with external partners while actively implementing protocols to protect intellectual property, vet participants, and prevent the unauthorized transfer of data and expertise.

EXPLOITATION TACTICS

CATEGORY 1: Financial Exploitation Tactics

These tactics involve an adversary using financial lures to gain access, influence, or ownership over DoW-related research and technology.

Adversary Approach	Risk Scenario	Who Is Targeted?
Grants and Sponsorship Offers	FIEs use shell companies or front "institutes" to offer lucrative grants, often with few milestones. This provides a legitimate-looking reason to engage with the research team. Be suspicious of sponsors who offer significantly above-market funding for early-stage research but insist the arrangement remain strictly confidential.	▪ Academic partners ▪ R&D personnel within DoW and the broader US Government
Venture Capital and Seed Funding	Adversaries establish or use opaque venture capital firms to invest in tech startups founded by former DoW or academic researchers, gaining board seats or access rights. A major red flag is an investment firm with a complex web of holding companies that is unusually focused on unclassified DoW projects.	▪ Defense industry innovators ▪ Academic partners
Joint Ventures and Corporate Partnerships	An FIE may propose a joint venture with a university lab or a defense contractor, contributing funding in exchange for access to facilities, data, or IP rights. Scrutinize partners who demand the use of their proprietary servers hosted overseas for joint data processing and analysis.	▪ Defense industry innovators ▪ Academic partners ▪ R&D personnel within DoW and the broader US Government

CATEGORY 2: Non-Financial Exploitation Tactics

These tactics exploit the academic and professional norms of collaboration and peer review to build trust and elicit information without a direct financial exchange.

Adversary Approach	Risk Scenario	Who Is Targeted?
Speaking and Conference Invitations	Researchers receive unsolicited, highly flattering, all-expenses-paid invitations to speak at international conferences, often from unknown institutes, to get the target outside their secure environment. Be wary of generous honorariums to keynote conferences, especially in high-threat countries or from unrecognized sponsoring organizations.	▪ Academic partners ▪ R&D personnel within DoW and the broader US Government ▪ Institutes and advisory bodies
Peer Review and Consulting Requests	FIEs will ask a target to review or consult on a project that is suspiciously similar to their own sensitive work, hoping to elicit corrections or insights. Avoid correcting errors in journals or consultations if doing so reveals unique methodologies used in your DoW projects.	▪ Academic partners ▪ R&D personnel within DoW and the broader US Government ▪ Institutes and advisory bodies
Visiting Scholar and Talent Programs	Adversaries use state-sponsored talent recruitment programs or visiting scholar arrangements to place witting or unwitting collectors inside university labs or R&D facilities. This often manifests as a visiting researcher presenting a resumé from a civilian university while hiding an undisclosed affiliation with a foreign defense-linked institution.	▪ Academic partners ▪ R&D personnel within DoW and the broader US Government ▪ Institutes and advisory bodies

CATEGORY 3: Defensive Practices and Reporting

This category outlines the defensive mindset and procedural actions required to mitigate the threats identified above. Secure collaboration is the goal, not isolation.

Adversary Approach	Risk Scenario	Who Is Targeted?
Initial Vetting and Due Diligence	Before any engagement, conduct open-source research and effective entity due diligence. Do not take a curriculum vitae (CV), business card, or website at face value, and always work with your security office to independently verify a partner's academic and professional history before signing an Nondisclosure Agreement (NDA).	▪ All defense research community members
Establishing Boundaries	Clearly define and document the scope of any collaboration in writing. This includes defining what data will (and will not) be shared, assigning who retains IP rights, and creating secure, segregated network drives so partners cannot access your entire research library.	▪ Defense industry innovators ▪ Academic partners ▪ R&D personnel within DoW and the broader US Government
Incident Reporting	If a red flag is identified (e.g., opaque funding, undisclosed affiliations), the engagement must be paused and the details reported immediately to the proper authorities. Never confront the individual directly; instead, forward suspicious communications to your CI Representative or security office.	▪ All defense research community members

OFFICIAL NCSC REFERENCE RESOURCES

For additional information on threat awareness materials or publications, consult these official channels:

- National Counterintelligence and Security Center (NCSC)
- NCSC Safeguarding Science Initiative
- NCSC Secure Innovation Guidance