WHO SHOULD BE VETTED?

Non-immigrant students and visiting scholars associated with:

- Foreign military research or institutions
- Foreign government sponsorship
- Foreign government or military employment
- Scholarship requirements mandating internships with defense companies or contact with foreign diplomatic institutions
- Academic exchange agreements involving emerging or dual-use technology
- International cooperative programs for innovative talents and foreign influence
- Cultural Institutes

REPORTING REQUIREMENTS

Code of Federal Regulation (CFR) 32 Part 117, National Industrial Security Program Operating Manual (NISPOM) requires reporting suspicious contacts, behaviors, and activities.

If you suspect you or your company have been targeted, report it immediately. Recognizing and reporting indicators is critical to disrupting counterintelligence (CI) threats and mitigating risks.

BE ALERT! BE AWARE!

Report suspicious activities to your facility security officer

DCSA
https://www.dcsa.mil

DCSA, Counterintelligence and Insider Threat Directorate
https://www.dcsa.mil/mc/ci

Center for Development of Security Excellence
https://www.cdse.edu

FOREIGN VETTING IN CLEARED ACADEMIA

**Defense
Counterintelligence
and Security Agency**

WHAT IS THE RISK TO ACADEMIA?

Proper vetting of foreign students, foreign faculty, and visiting foreign researchers/scholars is essential to protecting vital research and development within U.S. academic institutions. Enhanced vetting efforts play a vital role in thwarting adversarial acquisition of research conducted at U.S. academic institutions. This job aid will educate and assist cleared academia on threats from foreign entities.

POTENTIAL IMPACTS:

- National security implications
- Enhanced threats against the warfighter (our loss is their gain)
- Loss of federal and state research funding
- Loss of intellectual property revenue
- Loss of endowments, gifts, donations, prestige, or loss of credit
- Loss of grants and contracts
- Regulatory fines, penalties, and criminal liabilities

WHO IS BEING TARGETED?

U.S. academic institutions, specifically U.S. Government Affiliated Research Centers and Federally Funded Research and Develoment Centers, persist as a target of non-traditional collection of research and technology.

WHAT IS BEING TARGETED?

Information collection via academia allows adversaries to identify dual-use technologies and transfer proprietary research. Foreign adversaries continue to exploit the openness of U.S. academia and ongoing research as a means to transfer classified, unclassified, and controlled unclassified information (CUI) and sensitive, export-controlled research to advance national security interests.

COUNTERMEASURES

· Use security/red-flag and export control lists to screen for restricted or denied parties, such as the Consolidated Screening List, located at **www.trade.gov/consolidatedscreening-list**. Any dealings with a party on these lists violates U.S. export/sanctions regulations and requires further authorization and approval from the respective government agency:

> » **Denied Person List:** Individuals and entities denied export privileges

> » **Unverified List:** End users Department of Commerce (DoC) is unable to verify

> » **Entity List:** Parties whose presence in a transaction can trigger a license requirement supplemental to those elsewhere in the Export Administration Regulations

> » **Military End User (MEU) List:** No license exceptions are available for exports, re-exports, or transfers (in-country) to listed entities on the MEU List

> » **Nonproliferation Sanctions:** Parties sanctioned under various statutes

> » **Arms Export Control Act (AECA) Debarred List:** Entities and individuals prohibited from participating in defense articles export

> » **Specially Designated Nationals List:** Parties who may be prohibited from export transactions based on the Treasury's Office of Foreign Assets Control (OFAC) regulations

· If an individual or entity appears on these lists, contact your assigned DCSA CI Special Agent immediately

· Leverage vetting support from supporting Federal agencies. *Note: for non-U.S. persons only*

· Participate in the National Defense - Information Sharing and Analysis Center (ND-ISAC) to support identification and sharing of risk indicators

· Use publicly available information about foreign entities of concern to understand the potential risk of affiliations

· Scrutinize Curriculum Vitae (CV), resumes, and applications for red flag issues:

> » False information

> » Links to denied party screening indicators

> » Similar or identical information to other applicants

> » Affiliations with foreign military research or institutions from high-threat countries

> » Research interest mismatches between applicant's declared interest and what reflects in the CV

· Review applicant's research publications for red flag issues using web resources

> » Research topic conflicts between expressed interest and published work

> » Military-related research topics and applications

> » Coauthors affiliated with high-threat countries and/or links to denied party indicators and institutions

· Verify applicant's references listed in the CV or application

· Verify applicants declared contracts, grants, awards, etc., via **www.researchgate.net/**

· Use the Student and Exchange Visitor Information System (SEVIS), **www.ice.gov/sevis**, managed by DHS Immigrations and Customs Enforcement (ICE), to report student and visitor information, including suspicious activity. This allows derogatory information on a student and/or visitor to be tracked and monitored throughout the United States

· Leverage relationships with local and regional officials from the DCSA CI, FBI, ICE and other federal law enforcement and security organizations for enhanced review and analysis of foreign applicants