REPORTING REQUIREMENT

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

If you suspect you/your company are targeted, report it immediately, which is critical to disrupting foreign intelligence threats and mitigating risks. Reporting allows us to share and address risks together. Report suspicious activities to your facility security officer.

DCSA
www.dcsa.mil

DCSA, Counterintelligence Directorate
www.dcsa.mil/mc/ci

Center for Development of Security Excellence
www.cdse.edu

FOREIGN VETTING IN CLEARED ACADEMIA

BE ALERT! BE AWARE!

Report suspicious activities to your facility security officer

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

RISK TO ACADEMIA:

United States academic institutions, specifically U.S. Government Affiliated Research Centers within academia persist as a target of non-traditional collection and acquisition of fundamental research and essential technology. Solicitation and collection of vital information via academia allows adversaries to identify dual-use technologies and transfer proprietary research. Foreign adversaries will continue to exploit the openness of U.S. academia and ongoing research as a means to transfer classified, unclassified, and controlled unclassified information, as well as sensitive and often export-controlled research to advance their national security interests. Proper vetting of foreign students, foreign faculty, as well as visiting foreign researchers and scholars is essential to protecting the vital research and development that occurs within U.S. academic institutions. Enhanced vetting efforts will play a vital role in thwarting adversarial acquisition, whether witting or unwitting, of essential research conducted at U.S. academic institutions. This job aid will educate and assist cleared academia on the 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 (patents, copyrights, royalties)
- Loss of endowments, gifts, donations, prestige, or loss of credit
- Loss of grants and contracts
- Regulatory fines, penalties, and criminal liabilities

INDIVIDUALS TO BE VETTED:

Non-immigrant students and visiting scholars associated with:

- Foreign military research and/or institutions
- Foreign government sponsorship (i.e. China Scholarship Council)
- Foreign government and/or military employment
- Scholarship requirements mandating internships with defense companies and/or contact with foreign diplomatic institutions
- Academic exchange agreements involving emerging and/or dual-use technology
- International cooperative programs for innovative talents and foreign influence (i.e. Thousand Talents, Foreign Experts Programs)
- Cultural Institutes (i.e. Confucius Institute)

VETTING BEST PRACTICES:

- 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/consolidated-screening-list**. This list consolidates multiple export screening lists of the Departments of Commerce, State, and the Treasury. Any dealings with a party on any of these lists would violate U.S. export/sanctions regulations and would require further authorization and approval from the respective government agency:
  - **Denied Person List**: Individuals and entities that have been denied export privileges
  - **Unverified List**: End users who Department of Commerce's (DoC) Bureau of Industry and Security has been unable to verify in prior transactions
  - **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 that have been sanctioned under various statutes
  - **Arms Export Control Act (AECA) Debarred List**: Entities and individuals prohibited from participating directly or indirectly in the export of defense articles, including technical data and defense services
  - **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 there is a hit with respect to the screening of any individual or entity, contact your assigned DCSA CI Special Agent immediately.
- Leverage ***vetting support from supporting Federal agencies*** (DCSA, FBI, Military Services, NASA, DoE, DoC, etc.). Note: for non-U.S. persons only.
- ***Scrutinize Curriculum Vitae (CV)***, resumes, and applications for red flag issues:
  - False information
  - Links to denied party screening indicators (i.e. address, employment, references, etc.)
  - Similar or identical information with other applicants
  - Affiliations with foreign military research and/or institutions from high-threat countries
  - Research interest mismatches between applicant's declared interest and what reflects in the CV (i.e. applicant declared interest in a technology with a commercial/civil application but CV reflects a military application)
- Review applicant's ***research publications*** for red flag issues using web resources (Google Scholar, Research Gate, ORCID, Web Of Science, Dimensions)
  - 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 and/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 to include suspicious activity such as students not attending class, etc. This also 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 applicant