WHAT TO REPORT

Immediately notify your facility security officer if you observe any suspicious language or actions, or if you believe you were solicited by an ENC attempting to obtain information or technology they are not authorized to receive.

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

THREAT POSED BY EXPERT NETWORK COMPANIES

Defense Counterintelligence and Security Agency

WHAT IS THE THREAT POSED BY EXPERT NETWORK COMPANIES?

- Expert Network Companies (ENCs) (a.k.a Knowledge Brokers) connect subject matter experts (SMEs) with researchers, investors, or businesses seeking specialized insights and advice on industries, markets, or technical areas. These clients pay a premium to connect with experts who provide advice not otherwise available.
- ENCs act as a bridge between clients and experts, establishing a periodic, recurring, or continous relationship. ENCs are used by organizations seeking to gain knowledge quickly and make informed decisions.

WHO IS BEING TARGETED?

Cleared contractors, Department of Defense (DoD) service members, and former service members

WHAT IS BEING TARGETED?

- Electronics
- Optics and Lasers
- Radars
- Emerging Technology
- Space Systems
- Marine Systems
- Command, Control, Communications, and Computers
- Non-public Information on U.S. Government Policy

WHAT IS VALUABLE TO FOREIGN ADVERSARIES?

- Foreign governments aren't just interested in classified or export restricted information. Proprietary practices, supply sources, composition of materials, business methods, financial plans, or data handling are common requests through ENCs, some of whom are based in the United States.

HOW ARE YOU BEING TARGETED?

- ENCs offer cleared contractors, DoD service members, and former service members the opportunity to provide consultation for lucrative payment.
- ENCs connect the expert to undisclosed third parties, some being foreign individuals and organizations. Experts report being unable to ascertain the client's identity.
- While most ENC solicitations involve legitimate purposes, the nature of the process allows individuals or organizations to target technology and information while maintaining relative anonymity.
- Concealing the client's identity and keeping communications confidential creates an attractive environment for a Foreign Intelligence Entity (FIE). This poses a security vulnerability and allows a foreign adversary to take advantage of the purview provided by ENCs, obtaining information while maintaining anonymity.

HOW ARE EXPERTS FOUND?

- Professional networks
- Social media platforms
- Industry events and conferences
- Academic affiliation
- Referrals
- Publicly published material
- Experts seeking opportunities

HOW ARE EXPERTS CONTACTED?

- Social Media Requests
- Email
- Telephone Call
- Networking Sites
- Industry Events

HOW CAN YOU RECOGNIZE IT?

POTENTIAL INDICATORS OF FIEs

- Exceptionally high rates of pay per hour; payments in cryptocurrency and giftcards
- Offers to travel outside the United States
- Requesting information about a specific foreign government
- Requests to provide classified, controlled, or proprietary technology
- Requests for material support
- Bait and switch: requesting one topic, then changing to another
- Switching platforms outside the ENC
- Requests for personal information

COMMON FIELDS EMPLOYING ENCs

- Investment, Insurance, and Financial Services
- Medical Fields
- Electronics
- Manufacturing
- Security
- Government and Politics
- Business Strategy
- Aerospace Engineering
- Policy Development
- Economics

WHY DO COLLECTORS USE THIS METHOD?

It is cheaper for FIEs to illicitly obtain controlled unclassified information (CUI) or classified information and technology than to fund the initial research and development (R&D) themselves. The U.S. Government spends more on R&D than any other country in the world, making U.S. contractors performing R&D prime targets for foreign collection of classified and unclassified commercial technology.

VIGNETTE

A foreign company requests a wind tunnel modeling expert through an ENC and offers to pay them $X per hour. A professor specializing in wind tunnel modeling receives the solicitation, accepts the offer, and virtually meets with Company A for several hours, assisting them in managing the data. The expert is paid for their time and Company A can reach back out to that expert in the future for more assistance, establishing a working relationship.

"Foreign adversaries are leveraging LinkedIn in attempts to recruit both current and former Department of Defense (DOD) members, masquerading under the pretext of consulting, in a bid to gain strategic advantages in the great power competition."

Lt Col Lisenbee, Journal of Indo-Pacific Affairs, Air University, USAF