U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NRC's Defensive Counterintelligence Program and CI Awareness Briefing

TRTR Conference – San Diego, CA
September 17-21, 2017

Mr. Lance English - CI PM

Introduction

Welcome to the Defensive Counterintelligence and Awareness briefing. The purpose of this briefing is to acquaint you with the NRC's Defensive Counterintelligence (DCI) Program and provide an introduction to Economic or "Academic Espionage"

- Inform you about the threat economic espionage poses to the academic and business community

Objectives

By the end of this briefing you will be able to:

- Define "counterintelligence" & "academic espionage"
- Identify who targets academic staff and research, and how
- Explain how to recognize, mitigate, and report potential espionage activities
- Know what steps to take to prevent loss of academic research

Agenda

- Authority for Counterintelligence Program at NRC
- Definition of Counterintelligence (CI)
- Discuss The NRC's CI Program
- Targets and Impact of Foreign Intelligence Services (FIS)
- FIS Methodology; Spot, Assess, Develop, Recruit, Handle and Terminate
- Discuss Academic Solicitation
- Examples of Academic Espionage
- How to Report possible Espionage

Authority for CI Program: SECY-10-0158

The Staff Requirements Memorandum (SRM) SECY-10-0158, "Staff Options for a Potential Counterintelligence Program for Licensees Who Possess Uranium Enrichment Technologies and U.S. Nuclear Regulatory Staff," dated February 1, 2011, and a Chairman Tasking Memorandum, dated March 28, 2012, required the creation of a counterintelligence awareness training program at the NRC.

Counterintelligence programs aim to identify intelligence threats from state and non-state actors. As a defensive counterintelligence program participant, you can help the NRC focus efforts on preventing foreign actors from penetrating your institution and protect your research from foreign actors.

Definition of Counterintelligence

Executive Order (E.O.) 12333, "United States Intelligence Activities," as amended on July 31, 2008, defines counterintelligence (CI) as information gathered and activities conducted to identify, deceive, exploit, and disrupt or protect against:

- Espionage
- International terrorist organizations
- Other intelligence activities
- Sabotage
- Assassinations

CI is <u>NOT</u> physical security, personnel security, or information security.

The NRC's DCI Program

The NRC's DCI Program consists of two parts:

1. ***Internal Component:*** DCI training course, foreign travel pre-briefings and post-travel debriefings, foreign visitor and assignee vetting*, liaison with NRC offices, liaison with law enforcement and Intelligence Community agencies, and conducting internal DCI administrative inquiries.

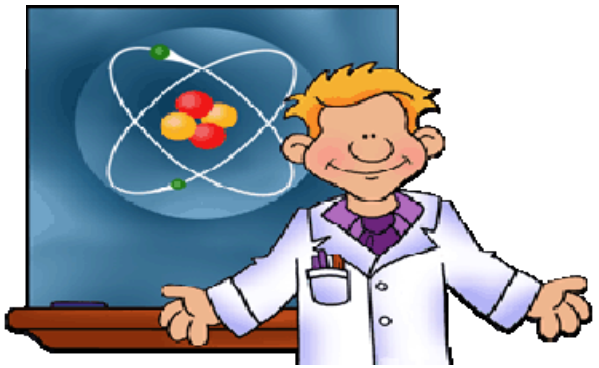
2. ***External Component:*** Leveraging Intelligence Community resources and DCI support and working closely with DCI programs at select fuel cycle facilities to develop and maintain the most effective DCI strategy.

*Note: The NRC's DCI Program does **not** conduct offensive counterespionage operations against suspected Foreign Intelligence Services (FIS).*

* Foreign visitor and assignee vetting is conducted by the Office of Administration, Division of Facilities and Security as described in Management Directive 12.1, "NRC Facilities Security Program."

Who Might Target the NRC or its Licensees?

- Friendly governments
- Hostile governments
- Foreign Intelligence Services (FIS)
- Foreign terrorist groups and sympathizers
- Domestic terrorist and anti-government groups
- U.S. Government employees and contractors
- Business competitors



Spies look like this…

…not this

Why are Academic Institutions Targeted?

U.S. Colleges and Universities have access to information that FIS, terrorists, and competing commercial industry are highly interested in such as patents, trade secrets, intellectual property and sensitive research.

FIS seek to:

- Minimize the military, political, or economic advantage of the U.S.
- Obtain technological parity or superiority
- Cause long-term, permanent damage to U.S. national security interests
- Enable terrorist activities
- Potentially disrupt U.S. critical infrastructure, including the domestic U.S. nuclear industry and the grid

What do FIS or Terrorists Want?

Below are some examples of what FIS and/or terrorists might want:

- Building floorplans and blueprints
- Dual use technology that may enhance military capabilities
- Radiological material, technology, or knowledge to create Radiological Dispersal Devices, Radiological Exposure Devices, or Improvised Nuclear Devices
- Emergency preparedness plans and procedures
- Computer passwords and login credentials
- Design Basis Threat information
- Contract or budget information used at nuclear power plants and fuel cycle facilities
- Training documents for the security forces at nuclear power plants and fuel cycle facilities
- Security and route information on transports

What do Economic Competitors Want?

Economic competitors may be interested in obtaining:

- New reactor designs
- New reactor design modifications, problems, remedies
- Classified and proprietary fuel enrichment technology
- Classified and proprietary fuel manufacturing technology and processes
- Supply chain information
- Contract information on guard force manning, budget, and security equipment

Note: FIS often have close and cooperative relationships with foreign economic competitors.

Foreign adversaries and economic competitors can take advantage of the openness and collaborative atmosphere that exists at most learning institutions in order to gain an economic and/or technical edge through espionage.

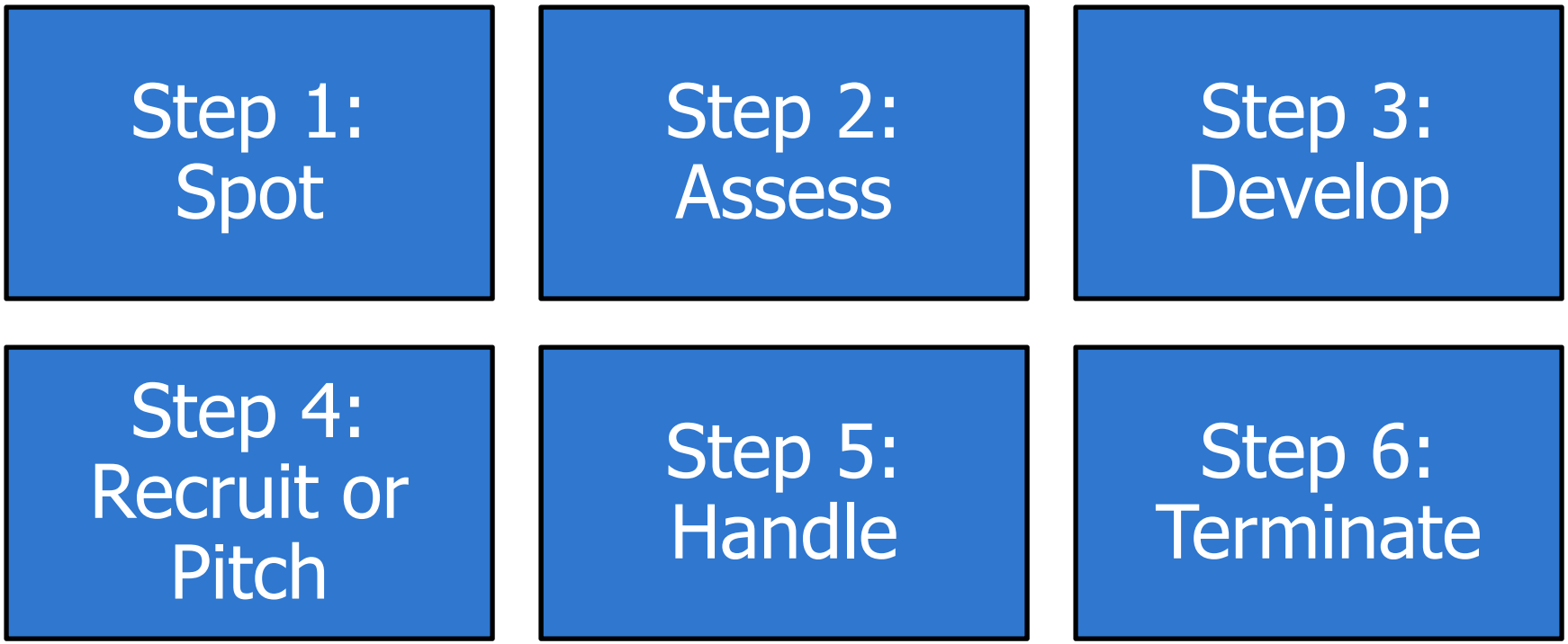
The Impact of Espionage

Espionage threatens the Nation's technical edge, military power, economic strength, and the ability to prevent the spread of nuclear technology which could be used to create weapons of mass destruction. Espionage can, or has resulted in:

- Loss or compromise of safeguards, classified, export control, sensitive but unclassified, and proprietary information
- Loss or degradation of U.S. weapons systems
- Increased risks to U.S. technological superiority
- Significant economic losses
- Loss of life

How do FIS Target and Recruit?

FIS Recruitment Methodology



Step 1: Spot

Identifying a person who might have information or access to information that FIS is interested in.

- If you are a FIS intelligence officer (FIS-IO) or an industrial competitor looking to acquire information especially on commercial nuclear information, you will go to the NRC or Academia to find it.

Step 2: Assess

The FIS-IO determines what you know and who you are to see if you may be valuable to them to develop and recruit. The FIS-IO is often, but not always, a foreign contact.

- This assessment can be done by eliciting information from you during casual conversation; from friends and co-workers; using social media such as Facebook, LinkedIn, Twitter; trade shows; professional venues; conferences; training courses; etc.
  - *It is important to know how much and what information you put out about yourself on social media forums and during conversations at public interactions like conferences, training, etc.*
- This step also includes the assessment of your potential vulnerabilities for exploitation (e.g., financial issues, gambling, drug use, adultery, etc.).

Step 3: Develop

If the initial assessment reveals that you have information of interest or are in a position to access information, the FIS-IO or business competitor will develop a relationship with you.

- This relationship is designed to break down any resistance you may have about discussing work and sensitive information.
- The FIS-IO may use some of the following ploys to connect with you:
  - Requests for private meetings and discussions
  - Repeated questions about work, access to information, and contacts
  - Invitations to dinner
  - Expensive paid trip
  - Expensive gifts
  - Escort services
  - Introduction to a "friend"
  - Request for unclassified (public) information at first
  - Maintaining a relationship after an event/conference/training

Step 4: Recruit or Pitch

The FIS-IO completes the deal and gets the individual to agree to a formal relationship through which the individual commits espionage.

The recruit is most likely emotionally tied to the adversary. While there are often complex reasons why individuals engage in espionage, ***some*** reasons people have been recruited are:

- Money
- Love or lust
- Coercion (blackmail) or influence
- Ideology

Step 4 may start off by the FIS-IO getting you to provide publicly available information and advances to Sensitive Unclassified Information, Proprietary Information, and/or Classified Information.

Step 5: Handle

Once the FIS-IO has recruited an individual, it establishes tradecraft.

Handling is the Tradecraft term used to describe the rules the recruited individual learns and follows to set up covert meetings, communicate, and pass information.

Step 6: Terminate

When the recruited individual is no longer needed or of no use to the FIS-IO, they will terminate the contact.

- It may be as simple as breaking all contact with the individual or as extreme as allowing the individual to be arrested for engaging in espionage (e.g., spying).
- For political or operational purposes, the FIS-IO may simply cease all communications with a person who is committing espionage on their behalf.
- Usually occurs just before arrest.

Academic Solicitation

Technique: use of students, professors, scientists or researchers as collectors improperly attempting to obtain sensitive or proprietary information

Requests may originate from know or unknown sources including:

- Foreign Universities or Academic Centers; Individuals overseas or placed in the U.S.
- Quasi-governmental Organizations such as research centers and institutes

Academic Espionage Tradecraft: there are several possible indicators of academic espionage:

- Social media manipulation; using false identities to solicit sensitive information via the Internet
- Academic event solicitation; using a conference as an opportunity to solicit sensitive information in person
- U.S. researchers receive unsolicited emails from peers in their academic field soliciting assistance on fundamental and developing research or are invited to attend or submit a paper for an international conference
- Overqualified candidates seeking to work in cleared laboratories as interns
- Candidates seeking to work in cleared laboratories whose work is incompatible with the requesting individual's field of research
- Intelligence entities will send subject matter experts (SMEs) requests to review research papers, in hopes the SME will correct any mistakes
- Conducts research/studies at odd hours without a need or authorization (i.e. weekends, holidays, or relatively un-usual schedules)

Academic Solicitation (con't)

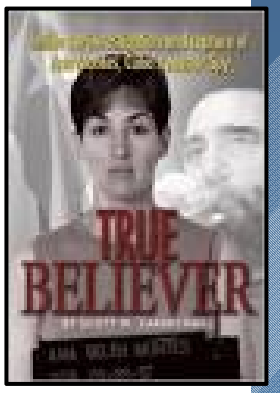
Countermeasures: The following countermeasures can protect against academic solicitation:

- View unsolicited academic solicitations with suspicion, especially those received via the internet
- Respond only to people who are known after verifying their identity and address
- If the requester cannot be verified or the request is suspicious:
  - ⇒ Do not respond in any way
  - ⇒ Report the incident to security personnel
- Ensure any response to known or unknown requestors includes only information authorized for release
- Make interns and visitors sign confidentiality agreements before they enter a laboratory.
- Keep laboratory logs up to date
- Put property marks on personal documents.

If you suspect you may have been a target of academic solicitation, report it.

Examples: Academic Espionage

Anna Montes



In 1984, a student-spy working for the Cuban intelligence service and studying at Johns Hopkins University "spotted" Ana Montes as a potential Cuban recruit. After being introduced to Cuban intelligence officers, Montes agreed to spy for Cuba while still a graduate student at Johns Hopkins. She later became an intelligence analyst at the Defense Intelligence Agency (DIA), focusing on Cuban issues. She was arrested in 2001 and sentenced to 20 years in prison.

Qinggiang Yin

In 2002, Qingqiang Yin, a former Cornell University researcher was arrested before boarding a flight to Shanghai from New York. He was carrying numerous bacteria samples and yeast cultures belonging to the university. The FBI investigation revealed Yin was seeking a job with a research facility in China and offered to bring the bacteria and yeast cultures to China for commercial enzyme production. He was sentenced to 12 months' imprisonment for conspiracy to defraud the U.S. government.

Cynthia Murphy

In 2012, the FBI arrested 12 deep-cover Russian SVR intelligence officers who were engaged in espionage against various American targets. One of the SVR officers was Cynthia Murphy, a.k.a. Lydia Guryeva, who while studying for a master's degree at Columbia University, was tasked by the SVR to develop relationships with classmates and professors who have or will acquire access to secret information and to report on their backgrounds and characteristics, providing assessments on their vulnerability for recruitment as spies.

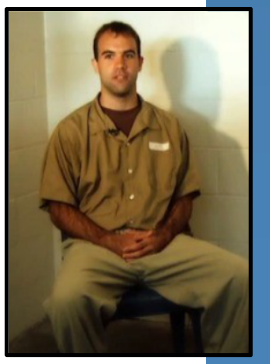
Examples: Academic Espionage

Hua Jun Zhao

In 2013, Hua Jun Zhao, a Chinese research assistant at the Medical College of Wisconsin, was arrested and charged with economic espionage after stealing cancer research compounds and shipping them to China, where he allegedly planned to take them to a Chinese university for further development. He pleaded guilty to the lesser charge of illegally downloading research data and was sentenced to time served (four-and-a-half months).

Glenn Duffie Shriver

Glenn Duffie Shriver spent over a year of his undergraduate studies living in Shanghai as part of a study abroad program. Just out of college and living in China, Shriver answered an English-language ad soliciting someone with a background in Asian Studies to write a paper on US/China relations concerning Taiwan and North Korea. Shriver met with a woman named "Amanda" who paid him $120 for his essay. Amanda introduced Shriver to two men who Shriver came to believe were Chinese intelligence officers who encouraged Shriver to apply for US State Department or CIA employment.



While Shriver studied for, applied, and tested for such employment, the MSS officers paid him a total of $70,000. Shriver was arrested and sentenced to four years' imprisonment after pleading guilty to conspiracy to commit unlawful conveyance of national defense information. Prior to his involvement with MSS, Shriver had no criminal history and by his own admission was acting out of greed and the lure of "easy money."

Report Your Observations or Concerns

Remember, ***YOU are the first line of defense against espionage!*** If you feel you are being solicited for information:

- Never feel obligated to answer questions that make you feel uncomfortable
- If a conversation is too probing with respect to your duties, private life, or coworkers, change the subject
- Be observant and take note of the person questioning you
- Maintain professional composure
- **REPORT, REPORT, REPORT** (ReportIt@nrc.gov); provide as much information as possible
- **DCI Program Manager**:

  Lance English, NSIR/DSO/ILTAB, 301-492-3006; lance.English@nrc.gov