UNM Industrial Security Department

Protecting UNM’s Most Valuable Assets

- People
- Research/PII
- Technology
- Reputation
NEW MEXICO – A TARGET FOR ESPIONAGE?

- Spaceport America + Federal Training Academies
- White Sands Missile Range
- Multi-National Conferences
- DoD and National Laboratories
- Cleared Companies
- Military Installations
- Public Research Universities

NEW MEXICO
• Protecting your research ensures that the work you have dedicated your life to is appropriately credited to you and not published or patented by other scientists or governments because your ideas or intellectual property were stolen either by a simple phishing email or while presenting at an international conference whether overseas or in the United States.

• You may be working on 6.1 research that has not yet been determined to be classified or export controlled information because potentially has military application.

• The Industrial Security Department is responsible for helping faculty, staff, and students with the security measures necessary to safeguard Classified, Sensitive, Intellectual Property, Export Controlled information, Controlled Unclassified Information (CUI) and Personal Identifiable Information (PII).

Contact 505-277-2058 or 277-2968 for assistance
INSTITUTIONAL CHALLENGE #1: FINDING A BALANCE

Research and Science
- Innovation
- Openness
- Dissemination of Knowledge

Protection of US Interests
- National Security
- Military Advantage
- Economic Advantage
WHY ARE CI & SECURITY IMPORTANT TO A UNIVERSITY?

CONTRACTS

• ENTRUSTED WITH DOD / ANOTHER COMPANY’S:
  -- INTELLECTUAL PROPERTY
  -- PII (CUSTOMER, EMPLOYEE)
  -- PROPRIETARY

UNIVERSITY OWNED

• INTELLECTUAL PROPERTY
• PROPRIETARY FORMULAS
• PROPRIETARY TECHNOLOGIES
• EXPORT CONTROLLED
• PII (CUSTOMER, EMPLOYEE)

NATIONAL SECURITY

• CLASSIFIED / CUI / FOUO / PII
• DEFENSE TECHNOLOGIES
• 6.1 RESEARCH THAT BECOMES BATTLEFIELD TECHNOLOGIES
ACADEMIA CHALLENGES

Compared against a typical U.S. cleared company, academic institutions/faculty members typically have a higher volume of contact with foreign nationals

Universities are awarded a large number of basic research grants; however, participants sometimes forget that their research may have military application
What is Academic Solicitation?

- Use of students, professors, scientists or researchers to improperly attempt to obtain sensitive or classified information through unsolicited requests for peer or scientific board reviews of academic papers or presentations; requests to study or consult with faculty members; requests for access to software and dual use technology.

- It is difficult to discern the legitimate contacts from nefarious attempts to gain access to information

- Fastest growing method of stealing your research

Who is being targeted?

- Subjected matter experts teaching technical courses

- Faculty and students conducting classified and Export Controlled research on behalf of a US Government sponsor

- Faculty, students, and subject matter experts with unclassified work published in scientific or technical journals or presented at international science conferences both outside and inside the US.

What is being targeted?

- Classified, sensitive, or export restricted basic and applied research

- Developing defense or dual use technologies
Method of Operation: Academic Solicitation

Top Targeted Technologies:
- Electronics
- Command, Control, Communication, & Computers
- Aeronautics
- Software
- Marine Systems
- Armament & Survivability
- Optics
- Materials: Raw & Processed
- Radars
- Energy Systems

Top Methods of Operation:
- Attempted Acquisition of Technology
- Suspicious Network Activity
- Solicitation or Marketing Services
- Request for Information
- Seeking Employment
- Foreign Visit
- Exploitation of Relationships

Top Collector Affiliations:
- Commercial
- Government Affiliated
- Individual
- Government

ACADEMIA ESPIONAGE CASES

TAKASHI OKAMOTO [Economic Espionage]

- Spied for a Japanese company
- Lerner Research Institute (LRI) of the Cleveland Clinic Foundation
- Chief of a LRI team conducting Alzheimer’s research
- Stole research material, destroyed/sabotaged related materials
- Aug 1999: Okamoto fled to Japan, who refused to extradite him to U.S.

HIROAKI SERIZAWA [Economic Espionage]

- Co-conspirator with TAKASHI OKAMOTO
- Kansas University Medical Center, Kansas City, KS
- Molecular Biologist (1996-2001)
- Plea agreement: 3 years probation, fine + community service
- This theft ended the employer’s Alzheimer’s disease research ($2.5mil)

HUA JUN ZHAO [Economic Espionage]

- Researcher at the Medical College of Wisconsin
- Stole cancer research material; deleted research data from the network
  • Sent material to wife in China; *purported the research was his own*
- Sentenced to time served waiting for trial (4.5 months) and turned over to immigration authorities
<table>
<thead>
<tr>
<th>THOMAS BUTLER [Export Control Violations]</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Texas Tech University; Professor, a leading researcher on plague</td>
</tr>
<tr>
<td>• Illegally transporting biohazards to Tanzania and not reporting the holdings to Texas Tech</td>
</tr>
<tr>
<td>• Transported plague samples from the Tanzania to the U.S.</td>
</tr>
<tr>
<td>• Charged with 69 felonies and faces more than 400 years in jail</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>REECE ROTH [Export Control Violations]</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Spied for China (2004-2007)</td>
</tr>
<tr>
<td>• University of Tennessee; Professor, Electrical Engineering and Computers</td>
</tr>
<tr>
<td>• Honorary professorship at Shenzhen Campus, Tsinghua University</td>
</tr>
<tr>
<td>• Provided export controlled data to two Chinese students</td>
</tr>
<tr>
<td>• 1 Jul 2009: sentenced to 48 months in prison, 2 years supervision</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DANIEL SHERMAN [Export Control Violations]</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Co-conspirator with Reece Roth; spied for China (2004-2006)</td>
</tr>
<tr>
<td>• Linked to University of Tennessee’s Plasma Sciences Laboratory</td>
</tr>
<tr>
<td>• Conspired with Reece to illegally export data via two Chinese students</td>
</tr>
<tr>
<td>• 10 Aug 2009: Sentenced to 14 months in prison</td>
</tr>
</tbody>
</table>
SUSPICIOUS CONTACT REPORTING

Report all unexpected contacts and requests for:

- Lecture overseas or in U.S. at an international conference
- Host a foreign national visit
- Review a CV for possible employment/study opportunity
- Relationship outreach
- Request for information
- Review a thesis or conduct peer research
- Ensure all sales and marketing requests are handled per company policy.
- Improper sales and marketing requests could easily circumvent export control policies and/or government regulations.
- Frequent international traveler, be wary of repeat accommodations. Collectors will place individuals in rooms that are “bugged” or otherwise under some type of surveillance.
• You can be the target of a foreign intelligence at any time or any place but the risk is greater when you travel overseas.
• Many hotel rooms overseas are searched and under surveillance.
• In a world where reliance on technology continues to grow, foreign entities have increased the targeting of laptops and cell phones.
• Conversations on your laptop and cell phones may be monitored.
• Installation of malicious software on computers.
• Get through crowded areas as quickly as possible.
TIPS FOR FOREIGN TRAVEL

• Leave unneeded electronic devices at home
• Remove all sensitive or exploitable information
• Use temporary email addresses not associated with UNM
• Perform an anti-virus scan prior to departure and upon return
• Encrypt data, hard drives and storage devices whenever possible
• If they take your computer out of your sight at customs, assume your computer has been compromised
• Do not take thumb drives at conferences
• Get a travel briefing from Industrial Security prior to departure
FOREIGN TRAVEL BRIEFINGS

• Country specific
• Country prohibitions  (Iran)
• Export Control Precautions
• Export Control Memo’s for equipment
• Licenses (Cuba)
• Safety and Security
• Health Recommendations/Health Insurance
• Classified/Unclassified
Elicitation:

Strategic use of conversation to subtly extract information about you, your work, and your colleagues

• Never underestimate the value of the information you are sharing
• Collectors pose as attendees, exhibitors, or scientists.

Reportable behaviors you may experience:

• Offers to act as a foreign sales agent
• Steering conversations or insistent questioning outside scope
• Taking excessive photographs of systems displayed at presentation or boots
• Asking personal questions to build a relationship for follow-up emails and on-going contact
• Multiple individuals simultaneously asking questions

CONFERENCES AND TRADE SHOWS VULNERABILITIES: WHETHER OVERSEAS OR WITHIN THE U.S.
I told her I was a Pitbull.
Phishing emails are looking more real - IT blocks 1-3 million phishing/spam emails daily

- Do not click on links or attachments from suspicious looking emails
- Hover over links or return paths to determine real destination
- Look for a sense of urgency, spelling errors, poor grammar, warning that you have been a victim of fraud
- Use same precautions on your mobile device as you would on your computer – download anti-virus software

Rule of thumb: Anytime you are asked for personal information, username or your password – it is a scam

Forward to spamdrop@unm.edu so Information Security can prevent others from getting it.
• INFORMATION SYSTEMS
  • Software/Hardware, Transmission
  • Systems, Modeling and Simulation, Information Communication Intelligence Systems, Information Security Systems

ALSO INCLUDED
  Aeronautics
  Space Systems
  Marine Systems
  Materials
  Guidance/Navigation/Vehicle

ELECTRONICS
  Microelectronics, Fabrication equipment, Electronic Materials, Components/Microwave Tubes, Microelectronics, Nanoelectronics

ARMAMENTS & ENERGETIC MATERIALS
  Missile Systems, Warhead Technologies, Survivability Armor and Warhead Defeat Systems

SENSORS & LASERS
It is imperative for academics to be familiar with, and comply with the laws, regulations, and procedures governing the restrictions of sharing classified, or export controlled technologies and information with foreign students or academics.

Imprisonment (10 years per violation)
Fines ($1 Million per violation)
Denial of Export Privileges
Loss of contracts above the $25,000 threshold
Career in Ruins

The type of enforcement action depends primarily on the nature and scope of the violations.
Never advertise your clearance to anyone, including your friends, neighbors, or family.

- 80% of adversaries’ information is collected through open sources
  Why are open sources valuable? They can piece the puzzle together…
  Why are you ignoring the green wire?
- Foreign national visitors
- Social networking sites (LinkedIn, Facebook, Twitter, Yammer)
- Foreign travel
- Conferences overseas or international conferences in the U.S.
Why Does UNM Need An FSO?

- FSO For Main And HSC
- TS Facility Clearance
- UNM is a Cleared Defense Contractor (CDC)
- CDC’s Must Follow National Industrial Security Program (NISP) Regulations
- Conduct Self-inspections Prior To Annual Security Vulnerability Assessments
- Liaison With Federal Agencies (DOD-DSS, FBI, DHS)
- Liaison With SNL, LANL, AFRL, DTRA….
- Suspicious Contact Reporting

Key Management Personnel

- President
- HSC Chancellor
- Provost
- FSO

Purple Arrow (NMCIWG)

- DSS
- FBI
- HSI
- DTRA
- OSI (Air Force)
- NCIS (Navy and Marines)
- 902nd Military Intelligence (Army)
- SNL, LANL
- U.S. Attorney’s Office

WHY IS UNM SO SUCCESSFUL?
In 2016, UNM received the **Cogswell** and **Counterintelligence** Awards from the Department of Defense.

- Only university to receive both awards
- Last 4 DOD security inspections – SUPERIOR rating
- Boast to get more Government contracts
INDUSTRIAL SECURITY & EXPORT CONTROL

Services

• Ensure Research Is Conducted Through Compliance With Federal Laws

• **Consult With Faculty Who Are Considering Whether Or Not To Become Involved In Controlled Work**
  
  • Oversee Classified And Export Controlled Contracts To Ensure Compliance
    
    • International Travel Briefings
      
      • Security Training
      
      • Information Protection
      
      • Security Clearances

• Develop Technology Control Plans (TCP’s) For Export Controlled Research
OTHER TRAINING OFFERED

• Office of Industrial Security
  • Active Shooter/Workplace Violence
  • Cyber Security – Phishing: How Not To Become a Victim of Email Fraud
  • Social Networking Security
  • Laptop and Cell phone Security
  • International Travel Security
  • Identity Theft

Deb Kuidis
dkuidis@unm.edu
505-277-2058

• Office of Export Control
  • Export Controls and Academic Research
  • International Research and Collaboration
  • Export Control Scenarios
  • Export Controlled University Property (purchasing and surplus)
  • Export Controlled Software
  • Performing Controlled Research
  • Protecting Controlled Unclassified Research (CUI)

Krista Laybourne
klaybourne@unm.edu
505-277-2968