NSF Cyber Security Conference
FBI Counterintelligence Domain Program Briefing
History/ Evolution of the Program

• DECCA
  - Developing Espionage and Counterintelligence Awareness

• ANSI R
  - Awareness of National Security Issues and Response

• DOMAIN
Technology Development Life Cycle Time-Line

End of Acquisition Life

Technology Development

System Fielding

Operational Use

System Manufacture

System Test/Design

Military Value of Information

Low

High

Fundamental Research

Classification/SAP Information

Information

Availability

OPENNESS

Labs & Centers

Contractors

 Universities

Technology Lifecycle and Counterintelligence Exposure

Exposure

6.0-.1  6.2  6.3  6.4  6.5  6.6  6.7

Technology Development Life Cycle Time-Line

Military Value of Information

= Classified/SAP Information

Low

High
Major Strategy Elements Supported By Domain Program

- **Change Behaviors**
  - Of most serious foreign threats
  - Of exploited individuals/institutions

- **Reduce Opportunities**
  - Of adversaries to collect intelligence and conduct operations

- **Band Field Offices/Partners Together**
  - To devise and implement joint operational plans that cross boundaries

- **Transformation to Proactive Program**
  - Pursue foreign positive intelligence collection effort
Changing Counterintelligence (CI) Paradigm

- Shift from reactive to proactive operations
- Acknowledgement of new business realities ("The World is Flat")
- Development and advocacy of risk mitigation strategies vs. threat avoidance
- Pushing counterintelligence awareness out to the business/academic community
- Leveraging resources to mutual advantage
Holistic Approach to CI Risk Management

• Insure that all facets of security (physical, IT, personnel) are aware of counterintelligence issues and incorporate risk detection and mitigation into cohesive business strategy.

• Partnership between USIC and Private Sector to leverage resources to maximum benefit of nation.
Pitching Partnership

- Emphasis on Confluence of Interest
  - CI protection = Research protection
- Leveraging finite resources
  - Recognition that we are all short handed
- Encouraging dialog
- Building confidence/trust
  - Subject matter competence
  - No threat posture
  - Confidentiality
Academic Alliance

• Foster spirit of cooperation
• Establish a dialogue
• Share information
• Increase awareness
Academic Alliance

- National Security Higher Education Advisory Board (NSHEAB)
- College and University Security Effort (CAUSE)
National Security Higher Education Advisory Board (NSHEAB)

- Members include 16 university presidents and chancellors
- Chaired by Graham Spanier, President of The Pennsylvania State University
- Three meetings a year
- Other participants include:
  - National Science Foundation
  - Department of Commerce
  - Central Intelligence Agency
  - Department of Defense
NSHEAB Members

- The Johns Hopkins University
- UCLA
- Carnegie Mellon
- University of Washington
- Texas A&M
- Iowa State University
- University of Pennsylvania
- MIT
- Purdue
- West Virginia University
- University of Florida
- UNC – Chapel Hill
- University of Maryland
- The Pennsylvania State University
- University of Wisconsin
Mission of the NSHEAB

- Promote understanding
- Create a forum for mutual issues
- Provide advice on the culture of higher education
- Build on traditions of openness, academic freedom and international collaboration
- Discuss matters pertaining to national security.
What is the RTP SIG?

- RTP = Research and Technology Protection
- SIG = Special Interest Group
- The RTP SIG is a tool for Domain Coordinators to use to provide information to their Domain representatives

http://www.infragard.net
What is the RTP Special Interest Group?

- The RTP SIG is a tool the FBI utilizes to provide information to cleared Defense Contractors, private industry and academia. Domain Coordinators are your local FBI contacts.
  - Mission: to provide actionable and relevant information to cleared defense contractors, private industry and academia to better enable them to protect their research and technology.
Why we need the RTP SIG

- To provide information to the targets of foreign intelligence services and economic espionage that will help them become a tougher target.
- To increase reporting of Counterintelligence events.
InfraGard RTP SIG

Research and Technology Protection

Welcome to the Research and Technology Protection Special Interest Group (RTP SIG). The mission of the RTP SIG is to provide actionable and relevant information to cleared defense contractors, private industry and academia so that they are better able to protect their research, technology and information. While our main concern is the protection of classified information, the same principles can be applied to the protection of trade secrets and other intellectual property.

Quick Links

- Workforce Education
- Online Resources
- Publications

In addition to the wide array of information available on the InfraGard main site, the RTP SIG supplements that with information that we think will be helpful to the individual who has responsibility for protecting research and technology. The buttons provided above are a quick way to go directly to the most commonly referred to items. For example, in the Publications section you can:

- Learn more about the recently unsealed Foreign Economic Espionage indictment for stealing military trade secrets.
- Are you interested in learning exactly how and why other countries are targeting U.S. technology? Read the recently released Annual Report to Congress on Foreign Economic Collection and Industrial Espionage.
- Read what former FBI Counterintelligence Director Dave Clark has to say about information security.
Research and Technology Protection

Workforce Education

Best Practices

- The Arizona Tech Protect Council has provided an example of a threat matrix that can be used to consolidate suspicious activity. This matrix helps track trends that might reveal issues that would otherwise go unnoticed. Proper reporting to your Domain Coordinator and DSS is encouraged.

- This is a list of some suggested reasonable measures to take to better protect your research and technology. Created by the San Francisco Strategic Technology Task Force this checklist can serve as a starting point for more effective protection of your intellectual property.

- Program Protection Planning: Are you a program manager responsible for the security of a product or system? Read here about the Department of Defense’s approach to Program Protection Planning.

Protect your Workplace

Posters

The following Department of Homeland Security (DHS) posters provide guidance on physical and cyber security and how to report suspicious behavior, activity, and cyber incidents. If you would like, you can download all of the posters at the same time using the Download complete series link.
Online Resources

United States Government Websites

The White House – National Security Council
"The National Security Strategy" (March 2006)

Office of the Director of National Intelligence (ODNI)
A current source for ODNI information including:

- ODNI Speeches
  - Threat Assessments
- Press Releases
- Website Links
  - "The National Intelligence Strategy of the United States of America – Transformation through Integration and Innovation" (October 2005)
  - "Intelligence Reform and Terrorism Prevention Act of 2004"

Office of the National Counterintelligence Executive (NCIX)
A current source for NCIX information including:

- "National Counterintelligence Strategy of Unites States" (March 2005)
- "Annual Report to Congress on Foreign Economic Collection and Industrial Espionage – 2004"
- History of Counterintelligence - American Revolution into the New Millennium

National Intelligence Council
"Mapping the Global Future Report of the National Intelligence Council’s 2020 Project"

United States Senate Select Committee on Intelligence
Current information regarding Senate oversight of the United States Intelligence Community (USIC)
Membership: the application process for the RTP SIG website

- Must be a current InfraGard member
- Must have a need for information on how to protect research and technology
- Should have the capability to take action on the information provided to them
How do I access the RTP SIG?

By selecting the “I want to join Research and Technology Protection InfraGard” button you will be requested to answer 7 questions:

1. What is your full name and to what InfraGard chapter do you belong?
2. What is your organization and has it been awarded any classified contracts?
3. Do you have a security clearance?
4. Does your company maintain or develop processes, formulas or other things that might be considered intellectual property or trade secrets?
5. What is your title?
6. Please explain how your responsibilities pertain to protecting your company’s research, technology or trade secrets.
7. Would you like to be listed in the SIG directory?