

Coordinating with Law Enforcement



SSA Tom Winterhalter, FBI, Cyber Division

What the FBI cannot do

“We cannot investigate if we are not aware of the problem”

- FBI Director Robert S. Mueller, III

And...

The FBI must work within the framework of the law.
....which can take time.



The Risk Equation

Cyber Threats - Considerations

Risk = Threat x Vulnerability x Consequence

- **Threat:** Any person, circumstance or event with the potential to cause loss or damage.
- **Vulnerability:** Any weakness that can be exploited by an adversary or through accident.
- **Consequence:** The amount of loss or damage that can be expected from a successful attack.



FBI Capabilities

What the FBI can do

- Investigate
 - National and global
 - Combine technical skills and investigative experiences
 - Long-term commitment of resources
- Forensics (RCFL)
- Patterns and Links
- Bring national security concerns to the intelligence community
- Large amount of resources



FBI Resources

The FBI Cyber Division

- 56 Field Offices with Cyber Squads
- 75 FBI Legal Attaché Offices around the world
 - Africa – 9 - African continent
 - Americas – 17 - Includes North, Central and South America
 - Asia – 13 - Includes Asia, India, South East Asia, Pacific Islands, and Australia
 - Europe – 13 - Includes Europe as well as Iceland and Greenland
 - Eurasia – 13 - Includes Eastern Europe, Russia, Former Soviet Republics and Turkey
 - Middle East – 10 - Includes Pakistan and Afghanistan
 - If we don't have one ... we will work to get one.
- Cyber Trained Agents embedded with foreign police forces.
- Training provided to international law enforcement community.



FBI Response

What the FBI won't do

- Take over your systems
- Repair your systems
- Secure your systems
- Share proprietary information with competitors
- Provide investigation-related information to the media or shareholders
- In essence ... we will not further victimize the victim



FBI Offerings

- National Cyber Investigative Joint Task Force
- Cyber Action Team
- Groups that are focusing on key threats and trends
 - These groups consist of agents, officers, and analysts from different agencies
 - ICS/SCADA TFC – FBI, DHS, and OGA partnering together
- Establishing cooperative working relationships with regulatory groups and agencies
- We can provide briefings to your employees regarding economic espionage, counterintelligence, APT, etc.
- InfraGard



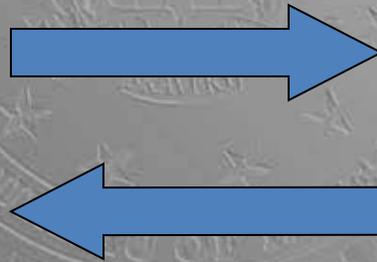
What is InfraGard?

- InfraGard is a partnership between the FBI and the public and private industry
- Includes business executives, entrepreneurs, military and government officials, computer professionals, academia, state and local law enforcement and concerned citizens
- It encourages sharing information between the government and the private sector for the purpose of **protecting the national critical infrastructure**



InfraGard and the FBI

Two way information flow



With the goal of protecting our Critical Infrastructures

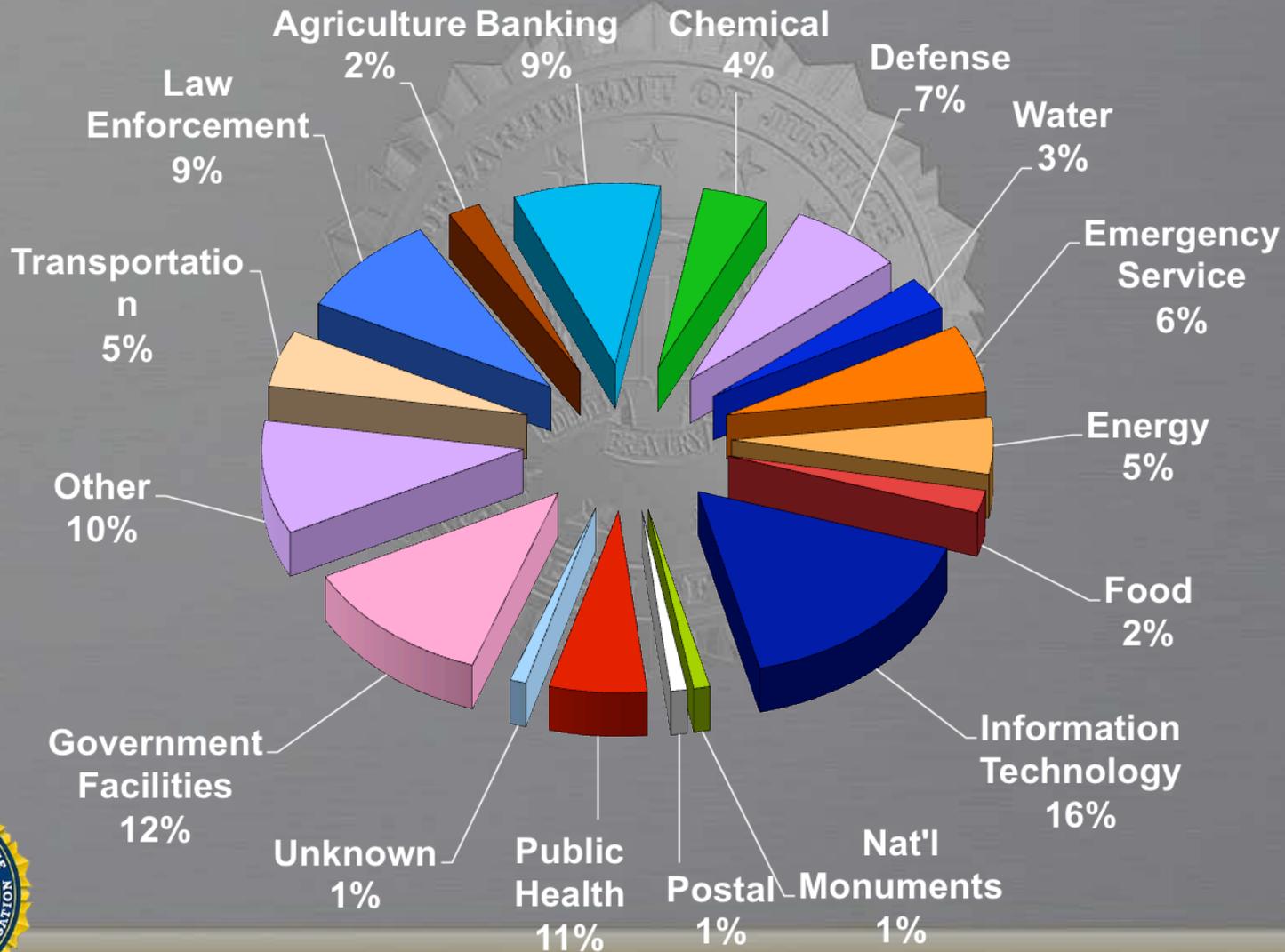


InfraGard's Mission & Goals

- Information sharing to reduce threats and vulnerabilities to critical infrastructures
- Develop and support a partnership with InfraGard members and the FBI to support ***all FBI investigative programs***



National Membership by Industry Sector



FBI Program vs Private Sector



- ▶ Provide vetting for membership
- ▶ Provide Secure Infrastructure
- ▶ Provide Law Enforcement Sensitive (LES) Intel Products
- ▶ Conduit for Investigations

MOU



- ▶ Self govern
- ▶ Identify Subject Matter Experts (SMEs)
- ▶ Provide non-government Intelligence
- ▶ Liaise with other Government Agencies
- ▶ Marketing/Fundraising
- ▶ Education



How is Information Shared?

- InfraGard uses a secure web site to communicate with members
- Website Contains:
 - Department of Homeland Security (DHS) threat alerts, warnings, and vulnerabilities
 - Intelligence Bulletins
 - FBI Agents assigned to each Chapter, bring meaningful news and information



FBI's Structure of InfraGard

- Supervised by the Public/Private Alliance Unit (PPAU), Strategic Outreach & Initiatives Section, Cyber Division
- Nationally, there are over 33,000 members comprising 86 InfraGard Chapters
- Each field office has a Special Agent InfraGard Coordinator who is a point of contact for the IMA and who recruits and vets new members
- Special Interest Groups



Why Should I Share Information with InfraGard?

- InfraGard provides an avenue to share information with a vetted membership that wants to help the FBI and get feedback
- Some of the members are experts in their field
- Members may see similar activity and report it to their local field office



How to Apply for InfraGard

- Visit the public website, www.infragard.net
- Click on “Become A Member”
 - Meet membership requirements.
- Fill out the application in a writeable pdf format and mail it to your local FBI Field Office or bring it to your Chapter Coordinator



Director Mueller at RSA

- **FBI Director Mueller at RSA:**

“No one country, company, or agency can stop cyber crime. A “bar the windows and bolt the doors” mentality will not ensure our collective safety. Fortresses will not hold forever; walls will one day fall down. We must start at the source; we must find those responsible.

“The only way to do that is by standing together. Together we can find better ways to safeguard our systems and stop those who would do us harm. For ultimately, we face the same threat. We both serve the American people. And we must continue to do everything we can, together, to minimize these attacks.”





Questions?

