

## **National Partnerships-National InfraGard**

### **Summary**

InfraGard is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a partnership between the Federal Bureau of Investigation and the private sector. InfraGard is an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States. InfraGard Chapters are geographically linked with FBI Field Office territories.

### **Background**

InfraGard is a Federal Bureau of Investigation (FBI) program that began in the Cleveland Field Office in 1996. It was a local effort to gain support from the information technology industry and academia for the FBI's investigative efforts in the cyber arena. The program expanded to other FBI Field Offices, and in 1998 the FBI assigned national program responsibility for InfraGard to the former National Infrastructure Protection Center (NIPC) and to the Cyber Division in 2003. InfraGard and the FBI have developed a relationship of trust and credibility in the exchange of information concerning various terrorism, intelligence, criminal, and security matters.

### **Goals and Objectives**

The goal of InfraGard is to promote ongoing dialogue and timely communication between members and the FBL. InfraGard members gain access to information that enables them to protect their assets and in turn give information to government that facilitates its responsibilities to prevent and address terrorism and other crimes.

The relationship supports information sharing at national and local levels and its objectives are as follows:

- Increase the level of information and reporting between InfraGard members and the FBI on matters related to counterterrorism, cyber crime and other major crime programs.
- Increase interaction and information sharing among InfraGard members and the FBI regarding threats to the critical infrastructures, vulnerabilities, and interdependencies.
- Provide members value-added threat advisories, alerts, and warnings.
- Promote effective liaison with local, state and federal agencies, to include the Department of Homeland Security.
- Provide members a forum for education and training on counterterrorism, counterintelligence cyber crime and other matters relevant to informed reporting of potential crimes and attacks on the nation and U.S. interests.

### **Description**

InfraGard is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a partnership between the FBI and the private sector. InfraGard is an

## *National Partnerships-National InfraGard*

association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States. InfraGard Chapters are geographically linked with FBI Field Office territories. Each InfraGard Chapter has an FBI Special Agent Coordinator assigned to it, and the FBI Coordinator works closely with Supervisory Special Agent Program Managers in the Cyber Division at FBI Headquarters in Washington, D.C.

While under the direction of NIPC, the focus of InfraGard was cyber infrastructure protection. After September 11, 2001 NIPC expanded its efforts to include physical as well as cyber threats to critical infrastructures. InfraGard's mission expanded accordingly.

In March 2003, NIPC was transferred to the Department of Homeland Security (DHS), which now has responsibility for Critical Infrastructure Protection (CIP) matters. The FBI retained InfraGard as an FBI sponsored program, and will work with DHS in support of its CIP mission, facilitate InfraGard's continuing role in CIP activities, and further develop InfraGard's ability to support the FBI's investigative mission, especially as it pertains to counterterrorism and cyber crimes.

Each FBI Field Office has a Special Agent Coordinator who gathers interested individuals to form a chapter. Any individual can join InfraGard. Local executive boards govern and share information within the membership. Chapters hold regular meetings to discuss issues, threats and other matters that impact their companies. Speakers from public and private agencies and the law enforcement communities are invited. The following illustrates additional activities that local chapters may offer:

- Training and education initiatives
- A local newsletter
- A Contingency Plan for using alternative systems in the event of a successful large scale attack on the information infrastructure

InfraGard members are represented nationally by an elected board of seven representatives called the InfraGard Board of Directors. Elections are held annually at the InfraGard National Congress for voluntary two-year terms. The Board is responsible for representing the membership in the partnership with the FBI. They conduct weekly conference calls to address a variety of issues that face the organization. Board members travel to various chapter activities and attend conferences promoting InfraGard and other issues pertinent to the program.

The Board established several committees to address issues such as membership, incorporation, and partnerships with other private sector association / organizations. Special Interest Groups (SIGs) have also been established to meet the challenges America faces in protecting against criminal, terrorist, and intelligence threats. One such SIG involves InfraGard, the National Institute of Standards and Technology (NIST), the Small Business Administration, and the FBI.

The InfraGard secure website provides members with information about recent intrusions, research related to critical infrastructure protection, and the capability to communicate securely with other members.

## *National Partnerships-National InfraGard*

### Requirements for Success

Key requirements for a successful InfraGard partnership would be to share actionable intelligence; to address issues involving economic and national security concerns and to work with a diversified group of U.S. based businesses, persons and entities, specifically designed to enhance engagement between the FBI and private sector, to secure funding through home agency supplemented by interagency agreements.

### Resources

National InfraGard has the following resources available through its partnership- A resources to help prepare for, respond to, and recover from disasters; web resources; and tools and templates.

[www.infragard.net](http://www.infragard.net)

### Training and Exercises

National InfraGard hosts and participates in joint training and exercises with the public and private sectors.

Each FBI Field Office has a Special Agent Coordinator who gathers interested individuals to form a chapter. Any individual can join InfraGard. Local executive boards govern and share information within the membership. Chapters hold regular meetings to discuss issues, threats and other matters that impact their companies. Speakers from public and private agencies and the law enforcement communities are invited.

### Communication Tools

National InfraGard uses the following methods of communication with their public/private sectors; email alerts; text message; in-person meetings; conferences and other events; newsletters; teleconferences; video conferences; website; media outreach; and public service announcements.

### Links

- **DHS/IAIP Daily Open Source Infrastructure Report**  
[Daily Report](#)
- **Internet Crime Complaint Center**  
[www.ic3.gov/](http://www.ic3.gov/)
- **Looks Too Good To Be True**  
[www.lookstoogoodtobetrue.com/](http://www.lookstoogoodtobetrue.com/)
- **BITS**  
[www.bitsinfo.org](http://www.bitsinfo.org)
- **The World Bank Group**  
[www1.worldbank.org/finance](http://www1.worldbank.org/finance)

## **National Partnerships-National InfraGard**

- **American Red Cross Homeland Security Advisory System Recommendations**  
[www.redcross.org/services/disaster/beprepared/hsas.html](http://www.redcross.org/services/disaster/beprepared/hsas.html)
- **Department of Homeland Security**  
[www.dhs.gov/](http://www.dhs.gov/)
- **SANS Institute Computer Virus Alerts and Warnings**  
[www.incidents.org/](http://www.incidents.org/)
- **U.S. Department of Justice - Computer Crime and Intellectual Property Section**  
[www.usdoj.gov/criminal/cybercrime/](http://www.usdoj.gov/criminal/cybercrime/)

### **Contact Information**

Verna D. Howard  
Management & Program Analyst  
Public/Private Alliance Unit  
[Verna.howard@ic.fbi.gov](mailto:Verna.howard@ic.fbi.gov)  
202-651-3219

### **DISCLAIMER**

FEMA's Private Sector Division of the Office of External Affairs facilitates information sharing and good practices for developing effective public-private partnerships. This Web site and its contents are provided for informational purposes only, without warranty or guarantee of any kind, and do not represent the official positions of the US Department of Homeland Security. For more information on the Private Sector Division, please email [FEMA-private-sector@dhs.gov](mailto:FEMA-private-sector@dhs.gov) or visit [www.FEMA.gov/privatesector](http://www.FEMA.gov/privatesector)