



# INFRAGARD

**An alliance  
for national  
infrastructure  
protection**

## **Partnership is our key resource**

As Americans, our lifestyle, economy, and national security are supported by a complex framework of businesses and services. The central role of these critical infrastructures and key resources (CIKR), however, makes them especially vulnerable as targets for both physical and cyber attack.

The Federal Bureau of Investigation's (FBI) priority programs share the common goal of protecting the nation's infrastructure and resources against threats posed by criminals and foreign adversaries. In support of their mission, Bureau teams including Cyber, Counterterrorism, Counterintelligence and others rely on close dialogue across government, but also benefit substantially from outside collaboration.

With the majority of infrastructure in the U.S. owned and operated by the public-private sector, cultivating information sharing partnerships that incorporate key industry stakeholders alongside law enforcement and government entities is crucial to protecting our most important public assets.

The FBI's InfraGard program provides a vehicle for seamless public-private coordination with government that expedites the timely exchange of information and promotes mutual learning opportunities relevant to CIKR defense.

## **Thousands of members, one mission: securing infrastructure**

The InfraGard alliance enlists the knowledge base and serves the interests of a wide range of private sector partners who own, operate, and hold key positions within some 85 percent of the nation's critical infrastructure.

With thousands of vetted members nationally, InfraGard's subject matter experts include business executives, entrepreneurs, military and government officials, computer security professionals, academia, and state and local law enforcement—each dedicated to contributing industry-specific insight and advancing national security.

While the FBI gains an improved understanding of the threatscape and a rich source of actionable intelligence through the organization, members are extended access to a host of information and tools that enable them to play a key role in securing infrastructure.

At the local level and online, program benefits encourage collaboration, improve threat awareness and preparedness, and arm members with vital information to safeguard their investments. Those who utilize benefits regularly are better equipped to identify, prioritize, and mitigate vulnerabilities, develop incident response plans, and enact the most current security best practices.



## InfraGard's evolution in progress

What began in 1996 as a cyber-focused collaboration between the FBI's Cleveland Field Office and information technology subject matter experts, local industry, and academia, has emerged two decades later as a full-scale, nationally-supported program. Today, each of the 80-plus InfraGard Members Alliances (IMAs) is geographically linked with one of the FBI's 56 Field Offices, and is represented jointly by its IMA leadership team and an FBI Special Agent Coordinator.

In 2003, the private sector members of InfraGard formalized InfraGard's non-profit, private sector corporate structure—the InfraGard National Members Alliance (INMA)—which oversees IMAs and allows them to engage federal, state, and local stakeholders in innovative programs outside the purview of the FBI.

InfraGard's liaison and outreach efforts have developed close working partnerships, not only between the private sector and the FBI, but with other pivotal agencies, to include the Department of Homeland Security (DHS), the National Institute of Standards and Technology (NIST), and the Small Business Administration (SBA).

Also as a result of the program, an agreement between the FBI Cyber Division, the FBI Weapons of Mass Destruction Directorate (WMDD), and the Naval Postgraduate School offers an exclusive training avenue for InfraGard members, which reinforces an understanding of government-private sector information sharing needs, security issues, and best practices.

**InfraGard provides a secure environment for the exchange of intelligence, strategy, and expertise among government agencies and the public and private sectors. The diverse partnerships forged through the alliance better equip us to disrupt criminal threats, prevent terrorism, and safeguard our communities.**

*FBI Director, James Comey*

## Defining our most important public assets

InfraGard engages subject matter experts and addresses threat issues across each of the 16 sectors of critical infrastructure and key resources recognized by Presidential Policy Directive-21, the Department of Homeland Security (DHS), and the National Infrastructure Protection Plan.

Critical infrastructures are those systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters, as defined in Section 1016(e) of the USA PATRIOT Act of 2001, 42 U.S.C. § 5195c(e).

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services and Banking
- Food and Agriculture
- Government Facilities
- Healthcare and Public Health
- Information Technology
- Nuclear Reactors, Materials, and Waste
- Transportation Systems
- Water and Wastewater Treatment Systems

Key resources are publicly or privately controlled resources essential to the minimal operations of the economy and government. The destruction of these individual targets would not endanger security on a national scale, but would create local disaster or profoundly damage national morale, as defined in Section 2(9) of the Homeland Security Act of 2002, 6 U.S.C. § 101(9).



## Member Benefits

Access to InfraGard's Secure Web Portal:

**[www.InfraGard.org](http://www.InfraGard.org)**

- Comprehensive suite of sensitive but unclassified FBI, Department of Homeland Security (DHS), and other federal, state and local threat intelligence products and daily news feeds
- Access to iGuardian, the FBI's cyber incident reporting tool designed specifically for the private sector
- FBI accredited website with 24/7 help desk and secure messaging promotes communication among members

Timely Intelligence Briefings and Analytic Products

- FBI and DHS threat advisories, intelligence bulletins, analytical reports, and vulnerability assessments in real time
- FBI and other government agency presentations to InfraGard chapters at member events

Unique Networking Opportunities

- Special Interest Groups (SIGs)
- Peer-to-peer collaboration across InfraGard's broad membership
- Information sharing and relationship building with FBI and law enforcement at all levels

Training and Education

- Naval Postgraduate School, Information Sharing Initiative (ISI) training program
- FBI, DHS, and other government security awareness training programs
- SANS Institute, local and online training and event discounts
- Free or discounted local seminars and conferences

### Membership Requirements

- U.S. citizen, 18 years or older
- Consent to and pass FBI security risk assessment and periodic recertifications
- Agree to adhere to InfraGard Code of Ethics and Information Sharing Policies



**To become a member visit [www.InfraGard.org](http://www.InfraGard.org)**

For more information contact [InfraGardTeam@InfraGard.org](mailto:InfraGardTeam@InfraGard.org)