# InfraGard Program

SA Gregory K. Baker
gregory.baker2@ic.fbi.gov
919-854-2400

**Federal Bureau of Investigation**

# What is InfraGard?

- InfraGard is a partnership between the FBI and private industry.
- It is a tool which encourages the sharing of information between the government and private sector for the purpose of national critical infrastructure protection.

# What is a critical infrastructure?

"Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

USA Patriot Act,

Section 1016(e)

# National Critical Infrastructures

"Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. These systems are so vital, that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States." *–President William J. Clinton, 1998*

Agriculture & Food, Banking & Finance, Chemical, Defense Industrial Base, Drinking Water and Wastewater Treatment Systems, Emergency Services, Energy, Information Technology, National Monument & Icons, Postal & Shipping, Public Health & Healthcare, Telecommunications, Transportation Systems

# Why does this affect private industry?

"Most critical infrastructures, and the cyberspace on which they rely, are privately owned and operated. The technologies that create and support cyberspace evolve rapidly from private sector and academic innovation. Government alone cannot sufficiently secure cyberspace."

National Strategy to Secure Cyberspace

# Is there a threat to the Critical Infrastructure?

Terrorist Organizations
State Sponsored Activity
Recreational Hackers
Hactivists
Organized Crime
Trusted Insiders
Foreign and Domestic Competitors
Lone Criminals
Information Warfare Units
The Unknown

# Critical Infrastructure Protection

- How do we protect or secure infrastructure, including cyber systems?
  - Reduce/Eliminate Vulnerabilities - education
  - Reduce/Eliminate Threats – information sharing
  - Reduce/Eliminate Consequences with planning
- Who protects the infrastructure?
  - #1, the owners & operators
  - FBI/Law Enforcement – investigation
  - DHS – threat warning and analysis
- It is no longer possible to separate our country's economic well-being from its national security

# What can be done?

- Identify, prioritize, and mitigate vulnerabilities
- Develop incident response plans
- Educate employees on best security practices
- Maintain audit logs
- Practice due diligence
- Report suspicious activity within organization
- Network with like-minded professionals
- Develop a relationship with law enforcement
  - Share information
  - InfraGard concept

# History of InfraGard

- InfraGard began in the Cleveland Field Office in 1996 as a local effort to gain support from the IT industry and academia for the FBI's investigative efforts in the cyber arena.
- In 1998, the FBI assigned national program responsibility for InfraGard to the former National Infrastructure Protection Center (NIPC); it was assigned to the Cyber Division in 2003.

# Changing Focus of InfraGard

- While under the direction of NIPC, the focus of InfraGard was cyber infrastructure protection.
- After 9/11/2001, NIPC expanded its efforts to include physical as well as cyber threats to critical infrastructures.
- The entire spectrum of American business and industry was now represented in InfraGard.

# InfraGard

- Overview
- Information sharing
- Special Interest Groups (SIGs)
- Membership

# InfraGard

*Overview*

# InfraGard Program Mission Statement

To support an information sharing partnership between the private and public sectors for the purpose of protecting the nation's critical infrastructures against attacks or failure caused by either foreign or domestic threats, and to support all FBI investigative programs, especially Counterterrorism, Counterintelligence, and Cyber Crime.

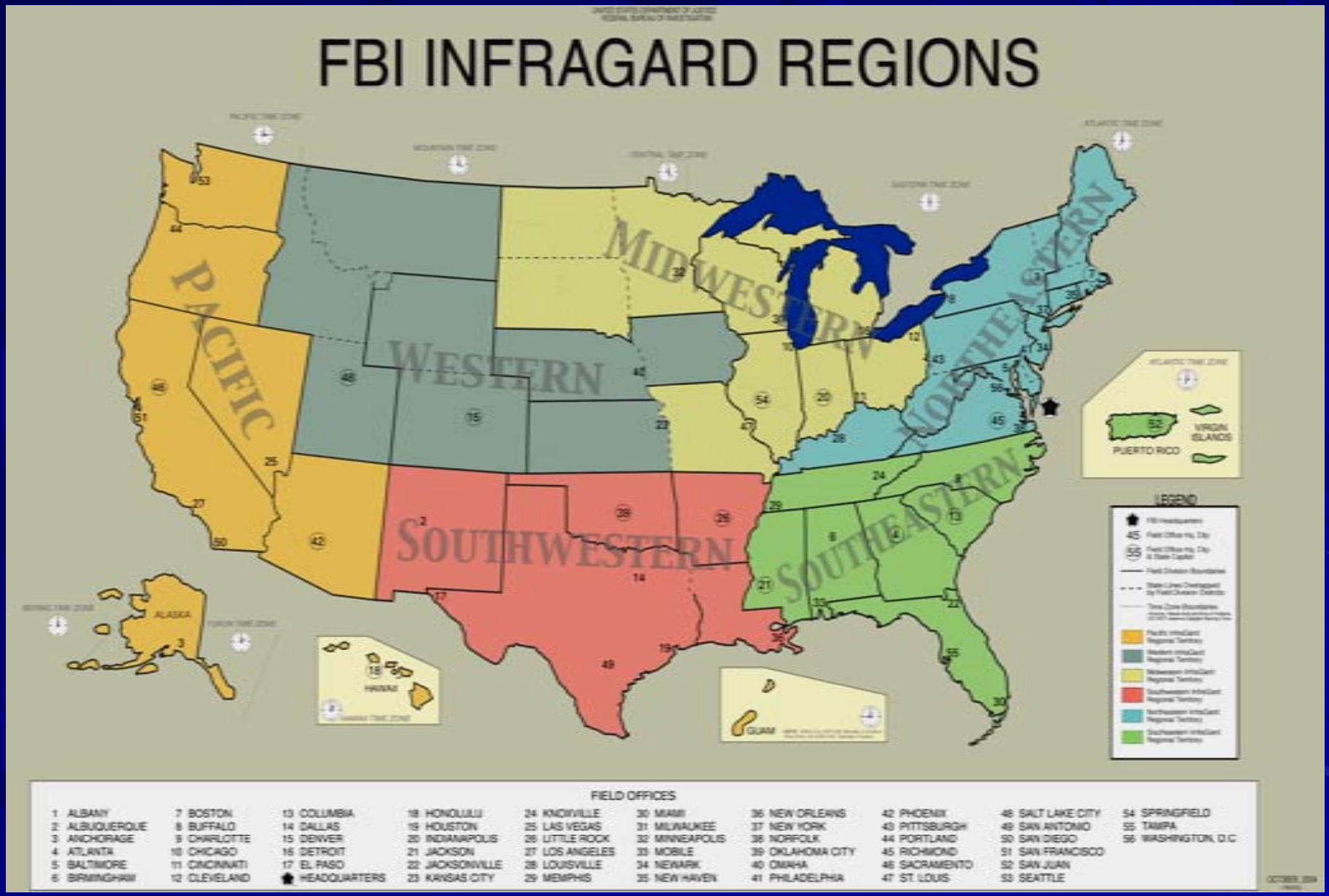
# Structure of InfraGard

- InfraGard falls under the Cyber Division at FBIHQ. It is part of the Information Sharing & Analysis Section, and the flagship program for the Public Private Alliance Unit.
- Nationally, there are over 26,000 members comprising 84 InfraGard Chapters, each led by a Special Agent Coordinator and a private industry InfraGard Members Alliance (IMA).
- 83 of the top 100 firms in the Fortune 500 have an InfraGard representative.

# Structure of InfraGard (contd.)

- InfraGard chapters are organized along the same geographic lines as local FBI field offices and resident agencies. Some field offices may have more than one chapter.
- The nation is also broken down into six InfraGard regions (see next slide).
- The private industry side of InfraGard is nationally headed by the InfraGard National Members Alliance (INMA). This is composed of a group of members elected by the presidents of each IMA to serve as the national governing board for the private sector.

# FBI INFRAGARD REGIONS




FIELD OFFICES

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 ALBANY | 7 BOSTON | 13 COLUMBIA | 18 HONOLULU | 24 KNOXVILLE | 30 MIAMI | 36 NEW ORLEANS | 42 PHOENIX | 48 SALT LAKE CITY | 54 SPRINGFIELD |
| 2 ALBUQUERQUE | 8 BUFFALO | 14 DALLAS | 19 HOUSTON | 25 LAS VEGAS | 31 MILWAUKEE | 37 NEW YORK | 43 PITTSBURGH | 49 SAN ANTONIO | 55 TAMPA |
| 3 ANCHORAGE | 9 CHARLOTTE | 15 DENVER | 20 INDIANAPOLIS | 26 LITTLE ROCK | 32 MINNEAPOLIS | 38 NORFOLK | 44 PORTLAND | 50 SAN DIEGO | 56 WASHINGTON, D.C |
| 4 ATLANTA | 10 CHICAGO | 16 DETROIT | 21 JACKSON | 27 LOS ANGELES | 33 MOBILE | 39 OKLAHOMA CITY | 45 RICHMOND | 51 SAN FRANCISCO | |
| 5 BALTIMORE | 11 CINCINNATI | 17 EL PASO | 22 JACKSONVILLE | 28 LOUISVILLE | 34 NEWARK | 40 OMAHA | 46 SACRAMENTO | 52 SAN JUAN | |
| 6 BIRMINGHAM | 12 CLEVELAND | ★ HEADQUARTERS | 23 KANSAS CITY | 29 MEMPHIS | 35 NEW HAVEN | 41 PHILADELPHIA | 47 ST. LOUIS | 53 SEATTLE | |

# What is InfraGard?

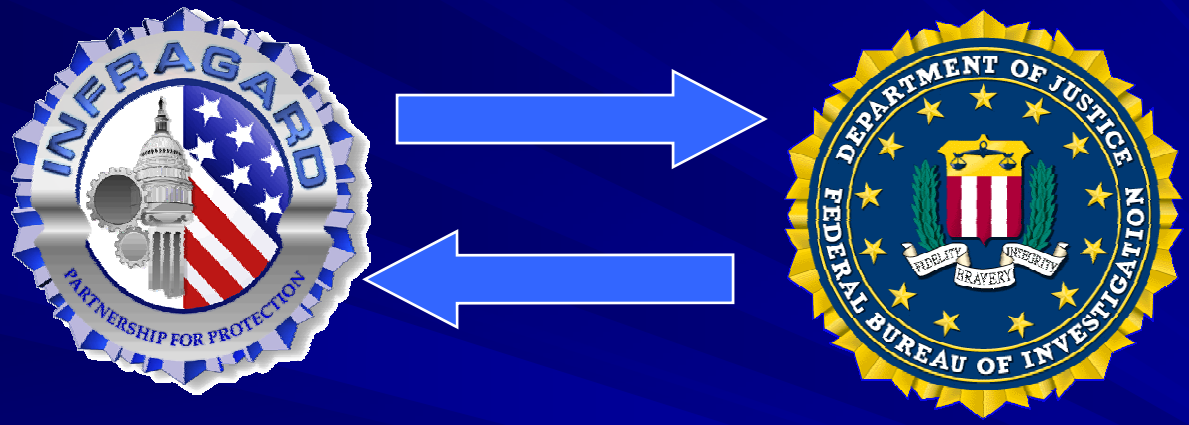
- Who: business executives, entrepreneurs, military and government officials, computer security professionals, academia, state and local LE, and concerned citizens
- Why: public/private partners share expertise, strategies, and information adding to intelligence and criminal cases

# What is InfraGard?

- www.InfraGard.net - public web site with DHS threat alerts, warnings, vulnerabilities
- Intelligence Bulletins from FBIHQ and Field Intelligence Groups
- Essence is information sharing, primarily from FBI Agents assigned to each Chapter, bringing meaningful news and information

# InfraGard and the FBI

Two way information flow




With the goal of protecting our Critical Infrastructures

# FBI Role in InfraGard

- Gathers and distributes intelligence
- Runs background checks and processes applications
- Organizes and facilitates both local and national InfraGard meetings
- Recruits new members

# The Role of Law Enforcement in Protecting Critical Infrastructures

- Law Enforcement reduces the threat
  - Primary mission is prevention
  - Secondary mission is to investigate after the crime occurs
- New era requires new solutions
- Law Enforcement has legal authorities and resources to determine who is behind an attack and stop them.

# Non-FBI InfraGard Roles

- Partners
  - National Center for Manufacturing Sciences
  - National Institute of Standards and Technology
  - Small Business Administration
- Board of Directors (7)
  - InfraGard National Member Alliance
  - Voluntary, two-year terms
  - Responsible for representing membership in their alliance with the FBI
- InfraGard Member Alliances – per each Chapter
  - An FBI Field Office may have more than one Chapter

# Non-FBI InfraGard Roles

- InfraGard Program Office (LSU)
  - Under contract with FBI to support InfraGard and Law Enforcement Online
    - Sustains InfraGard's ability to collect and disseminate information
    - Principal point of contact for daily operations
  - Significant assistance:
    - Processes member applications; assists with organizing training conferences; moderates 190 Listservs

# Non-FBI InfraGard Roles

- Formats and uploads daily public and secure web site content
- 24/7 technical support for members
- Administers InfraGard and LEO, reducing overall costs

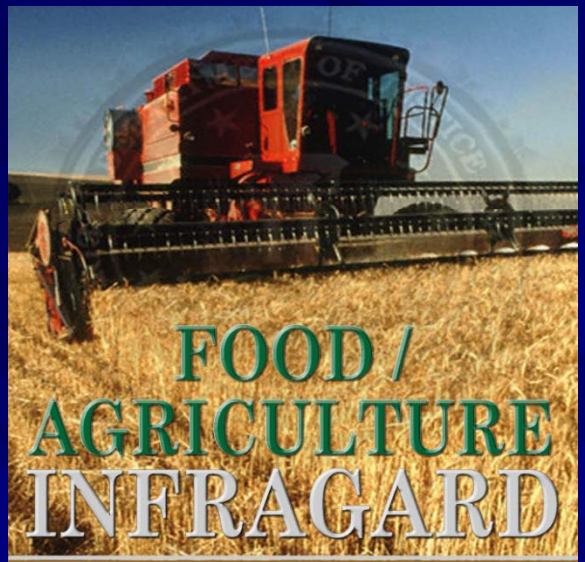
# Why InfraGard?

- Sharing of FBI & DHS information
- Protection requires assistance from owners and operators of critical infrastructures
- Computer and physical security expertise shared and enhanced
- Relationships help establish trust between private industry and government agencies
- Aids Law Enforcement and intelligence gathering

# What Chapters have done

- Philadelphia: CIDDAC – automated cyber attack early warning system prototype
- Las Vegas: aided investigation allowing LE to capture a criminal who used a computer to embezzle $150,000+
- Los Angeles: participated in a two-day nationwide simulated terrorist attack training exercise
- San Francisco: trained FBI Agents on hacker tools
- Vermont: offers free classes to teach local residents how to protect themselves from online threats
- Portland: Phishing authority added to FBI Subject Matter Expert alliance
- Little Rock:  Acxiom case – 6 convictions on intrusion case based on IG member referral

# Special Interest Groups



## FOOD / AGRICULTURE INFRAGARD

The Food/Agriculture InfraGard Special Interest Group (SIG) is a resource dedicated to the safeguarding of the food and agriculture sectors of both private industry and government through information-sharing networks and a private secure portal of communication. It is a collaborative effort of the Counterterrorism and Cyber Divisions of the FBI. The Food/Agriculture InfraGard SIG is intended to enhance the sharing of information among private sector stakeholders who can be called on to assist the FBI in detecting, deterring, assessing, and preventing threats and attacks targeting the food and agriculture sectors of our nation's critical infrastructures. It aims to be a consortium of agriculture security professionals and law enforcement officials with the common goal of protecting America's farmland, food products, animals, and industry.

Participation in the Food/Agriculture InfraGard SIG requires membership in the national InfraGard Program and affiliation with the agriculture industry. Visit www.infragard.net for national membership. Once a participant in the national program, a member may request access to the Food/Agriculture InfraGard SIG by submitting an e-mail containing answers to questions about his/her association with the agriculture industry.

Assessments, news, relevant links, and up-to-date information on protection issues related to the agriculture community are available to Food/Agriculture InfraGard SIG members. Members may submit articles for posting on the site, and communicate on the message board about food and agriculture sector issues in a secure environment. The site is also broken into areas specific to law enforcement, industry, food/agriculture agencies, animal/human health organizations and academia. The Food/Agriculture InfraGard SIG is a unique opportunity for you to belong to the fastest growing network dedicated to agriculture-specific information sharing, driven to protect the food and agriculture infrastructure of the United States. To belong to the Food/Agriculture InfraGard SIG, visit www.infragard.net. For questions, please contact infragardteam@infragard.org.

## CHEMICAL INFRAGARD

The Chemical InfraGard Special Interest Group (SIG) is a resource directed to the safeguarding of the chemical sector of both private industry and government through information-sharing networks and a private secure portal of communication. It is a collaborative effort of the Counterterrorism and Cyber Divisions of the FBI. The Chemical InfraGard SIG is intended to enhance the sharing of information among private sector stakeholders who may be called upon to assist the FBI in detecting, deterring, assessing, and preventing threats and attacks targeting the chemical sector of our nation's critical infrastructures. It aims to be a consortium of chemical security professionals and law enforcement officials with the common goal of protecting America's chemical plants and industry.

Participation in the Chemical InfraGard SIG requires membership in the national InfraGard Program and affiliation with the chemical industry. Visit www.infragard.net for national membership. Once a participant in the national program, a member may request access to the Chemical InfraGard SIG by submitting an e-mail containing answers to questions about his/her association with the chemical industry.

Assessments, news, relevant links, and up-to-date information on protection issues related to the chemical community are available to Chemical InfraGard SIG members. Members may submit articles for posting on the site, and communicate on the message board about chemical sector issues in a secure environment. There is also a Chemical InfraGard SIG listserv which allows SIG moderators the ability to correspond upcoming events and important announcements directly to SIG members via secure e-mail. The Chemical InfraGard SIG is a unique opportunity for you to belong to the fastest growing network dedicated to chemical-specific information sharing, driven to protect the chemical infrastructure of the United States. To belong to the Chemical InfraGard SIG, visit www.infragard.net. For questions, please contact infragardteam@infragard.org.

# Other SIGs

- Mass Transit
- Cyber Security
- Research Technology Protection

# Special Interest Group (SIG)

- A combined effort of the FBI Cyber Division and Counterterrorism to partner with the _____ Sector for communication, Information Sharing, and investigative purposes.

- Intended to enhance information sharing among public and private sector and subject matter experts who can be called on to assist in detecting, deterring, assessing, and preventing threats and attacks targeting the _____ sector of our nation's critical infrastructure.

# SIG

- Participation in the _____ InfraGard Special Interest Group (SIG) requires pre-vetted membership in InfraGard and demonstrated occupational interest in the _____ sector or currently employed by a law enforcement agency.

- The website has sector-specific assessments, news, related links and a message board, allowing members to communicate in a secure environment about protection issues related to the protection of the _____ sector.

# Food/Agriculture

mlitchfield | 03.08.06

Law Enforcement | Industry | Food/Ag Agencies | Animal/Human Health | Academia

Home > Food/Agriculture InfraGard

## Welcome to Food/Agriculture InfraGard

Welcome to the FBI Food and Agriculture Infragard (AgInfraGard) Web site. AgInfragard represents a combined effort of the FBI's Counterterrorism and Cyber Divisions to partner with the food and agriculture industry sectors for communication, information sharing, and investigative purposes. This Web site contains a number of features and links that provide information, as well as tools that provide interactive capabilities aimed at expanding the FBI's Food and Agriculture Outreach Program.
The partnership between the FBI and the Food and Agriculture sector is vital to FBI's Counterterrorism mission. The FBI welcomes your participation in the Web site and continues to look for new ways to expand the Food and Agriculture Outreach Program.

### Acknowledgment

The FBI CTD WMDCU would like to thank and acknowledge the FBI Field Divisions who have assisted in making AgInfraGard a successful initiative. Additionally, the FBI would like to thank the many participants from the food and agriculture industries who have assisted with the Food and Agriculture Outreach Program.

Agriculture Industry

Home
News
Publications
WMDCU Mission
FBI WMD Coordinators
Online Resources
Meetings/Conferences
Specialist
LES Guidelines
List-Serv
Contact Us

FBI Infragard protected information, to be disclosed only as needed for U.S. corporate security purposes.

# InfraGard

## Information Sharing

# Shared Problem = Shared Responsibility

"Most critical infrastructures, and the cyberspace on which they rely, are privately owned and operated. The technologies that create and support cyberspace evolve rapidly from private sector and academic innovation. Government alone cannot sufficiently secure cyberspace"

National Strategy to Secure Cyberspace

# How accomplished?

- Jointly with DHS
- Intelligence product for dissemination to InfraGard secure web
  - Produced by Analyst/Agent -- Field Intelligence Group – dissemination – FBIHQ to InfraGard
- InfraGard LES admonishments and accompanying question or statement
  - Assimilation of new information into intelligence or case work
- Electronic communication – FBI field office

# Information Sharing with DHS

# DHS Information Sharing

- FBI's National Infrastructure Protection Center (NIPC)
  - March 2003, Homeland Security Act transferred NIPC to DHS
  - former NIPC components kept for Cyber Division
    - InfraGard
    - National security and criminal Computer Intrusion Section
    - Special Technologies and Applications Section

# DHS Information Sharing

- DHS received NIPC's Analysis & Warning Section
  - Alerts and advisories
- FBI provides threat and vulnerability investigative information to help DHS fulfill its mission
- FBI has encouraged its InfraGard members to develop a close relationship with DHS
  - InfraGard's elected leadership regularly communicates with DHS

# DHS Information Sharing

- Intelligence community producing standardized intelligence products so information is shared
- FBI has formalized a process where real-time unclassified, sensitive intelligence is propagated to InfraGard members
  - Goal: timely input to add to intelligence or aid pending criminal matters from broad-based, vetted InfraGard members
  - Ongoing: intelligence shared with private sector on a case by case basis

# InfraGard

## Membership

# Why become a member of InfraGard?

- To demonstrate reasonable care and adherence to the best practices which can minimize liabilities
- To increase profitability or cost savings over the long term by reducing disaster recovery expenses

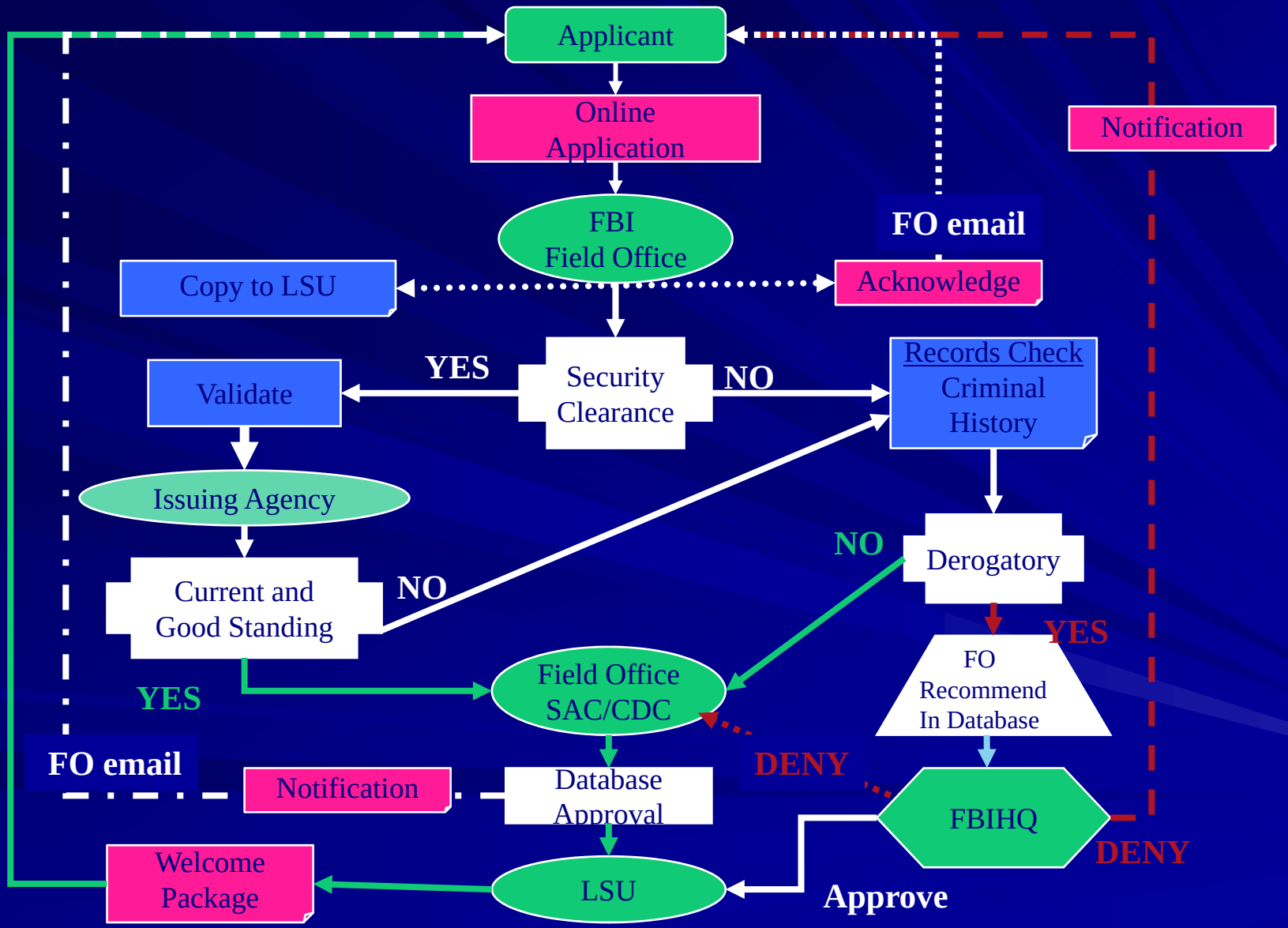
# Why become a member of InfraGard? (cont.)

- FBI Certified and Accredited System
- VPN Technology provided to user
- No cost to user
- Secure e-mail communication
- Host based virus scanning of e-mail
- Secure online information sharing environment:
  - Library articles
  - Periodicals
  - Alerts & Advisories
  - Sector-specific abstracts

# Who should join?

- You!! If you, your company or government agency supports the critical infrastructures
- Anyone who works for organizations that can assist in assessing vulnerabilities and minimizing risks
- Persons capable of accepting Law Enforcement Sensitive, unclassified information and providing feedback to aid criminal cases or intelligence gathering
- Good citizen

# InfraGard Application Process



# How to Apply for InfraGard

- Visit our public website, **www.infragard.net**
- Click on "***Become A Member***"
- Fill out the application in writable pdf format and either mail it in to your local FBI Field Office or bring it to your Chapter Coordinator

# What Happens Next?

- Once your application and background checks are processed, you will be sent notification of your membership status.
- If approved, you will receive a packet containing a Welcome letter, VPN software, a membership card, and a sheet containing your password, login ID, and InfraGard e-mail address.
- Once you receive your packet, call the InfraGard Technical Support Line (24/7) to enable your account.
- Once enabled, you can setup your e-mail, view the secure website, post to listservs and message boards, etc…

# Web Sites

- www.infragard.net – National Site
- www.ecinfragard.org – Eastern Carolina (RTP) Site
- www.ncinfragard.org – Charlotte Site

# Questions?

Presented by:

SA Gregory K. Baker

gregory.baker2@ic.fbi.gov

919-854-2400