THE FBI/INFRAGARD PARTNERSHIP

1996 - 2016

By Earl Motzer, Ph.D.

with editorial assistance from John F. Fox, Ph.D.

September 2016

InfraGard for almost two decades now has been at the core of the FBI's outreach to the private sector. It is an association of businesses, of academic institutions, law enforcement agencies, and others who are coming together to share information.

FBI Director James Comey July 7, 2014

Table of Contents

Acknowledgements

When I was elected Vice Chairman of the InfraGard National Members Alliance Board of Directors in late 2015, I suggested Board Members participate in a Gap Analysis exercise to determine priorities for our next twelve months of voluntary service for our 50,000 + members.

I had recently completed a project in Mercer County, Kentucky to research the elected Sheriffs since 1774 when the county was first established. The thought occurred to me that we will be celebrating the twentieth anniversary of InfraGard in 2016 and it would be nice to document the history of InfraGard and its partnership with the FBI while most of those involved were hopefully still alive and able to share information.

InfraGard began in Cleveland, Ohio in 1996 so I contacted the Society of Former Special Agents of the FBI (SOCXFBI). I had worked with that organization in a previous role as National President of the FBI National Citizens Academy Alumni Association. Nancy Savage, Executive Director of SOCXFBI, agreed to place a message in the organization's newsletter and, within four days, Robert Fiatal, the former FBI Cleveland Supervisor of the Foreign Counterintelligence/Terrorism/Computer Crimes Squad and current Ohio Assistant Attorney General replied. He was so helpful in putting me in touch with former FBI Special Agents and started the ball rolling.

FBI Cleveland InfraGard Coordinator Ganpat "Gunner" Wagh obtained approval from SAC Stephen Anthony for me to visit the Cleveland Field Office to gather information and interview both Intelligence Analysts and Special Agents who were involved at the time. Intelligence Analyst Anita Fjeldstad shared with me the Newsletters she wrote between 197 and 2000.

Bryan Hornick, the current InfraGard Northern Ohio Members Alliance President, invited me to attend a membership meeting and explain our history project and helped to connect me with former members.

Former FBI Special Agents who provided great assistance included Dave Lyons who followed Jerry Personen, the first InfraGard Coordinator who is now deceased, Brian Vigneaux and the SAC at the time, Van Harp. Teresa Personen, Jerry's widow, was very helpful to share photos and information. Former INMA President Sheri Donahue provided the listing of board members, officers and committee members. Former President Rob Schmidt shared the options to consider regarding the corporate governance legal issues and other important documents.

Two of the original volunteers were Dave Strothcamp, a computer security professional and Mike Daugstrup, a senior banking official. Both provided helpful information and Daugstrup gave me his old files which added many facts previously unknown.

Ed Napoleon, a senior banking official sent me some old files regarding options for naming of the organization and a picture of when then FBI Director Louis Freeh visited the Cleveland Field Office. Bob Heim, the then President of the Information System Audit and Control Association (ISACA) suggested the name Infraguard. Dave Strothcamp found Infraguard was already used as a software product and offered InfraGard which was adopted.

FBI SSA David Ford was working at the National Infrastructure Protection Center and gave me excellent information about the early decision of FBI Headquarters to transition InfraGard from a Cleveland based

organization to FBI Headquarters. He was followed by Brett Hovington who also provided assistance to the National Citizens Academy Alumni Association. Don Good followed Hovington in this transition role.

Regarding the transition, Dr, Phyllis Schneck, Rob Schmidt, Jeff Schmidt and Bill Yang, each in their own way, gave me valuable information and files.

Sheri Donahue was the first Managing Director of the InfraGard National Members Alliance and shared who was serving in what capacity over the years as well as the President's Handbook.

Thanks also to the volunteers who served as Chairs of the InfraGard National Members Alliance Dr. Phyllis Schneck, Dr. Kathleen Kiernan, Admiral David Pekoske and Gary Gardner, and Presidents Ronald Dick, Rob Schmidt, Dyann Bradbury, Sheri Donahue and Jerry Bowman.

Last but by no means least, John Fox, Ph.D., the FBI Historian, provided previously undiscovered information and valuable editing and guidance, and my wife Eileen for her understanding of the amount of time I devoted to this project.

Bottom line - I love the new friendships I made and very much appreciate the courtesy and cooperation received in this labor of love to highlight the government leaders and private sector volunteers who made history in initiating successful bi-lateral information sharing to help protect and maintain America's critical infrastructure resilience.

Earl J. Motzer, Ph.D.
August 2016

- CHAPTER ONE -

Critical Infrastructure Protection (CIP) & Electronic Crimes in America – the 1980s & 1990s

> "The United States is a society totally dependent on interlocking networks and nodes for communications, transportation, energy transmission, financial transactions and essential government and public services. Disruption of key nodes by terrorists could cause havoc, untold expense and perhaps even mass deaths. We are, in the jargon in the trade, a 'target rich environment.'"
>
> Senator Patrick Leahy (1990)

Critical infrastructure provides the essential services that underpin American society and serve as the backbone of the nation's health, security and economy. It refers to the electric grid, our water supply, our communication and transportation systems, and the buildings we occupy full time and/or part time.

There are currently sixteen critical infrastructure sectors: chemical; commercial facilities; communications; critical manufacturing; dams, defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology, nuclear reactors, materials and waste; transportation; water and waste water systems.

CIP THREATS

There are many things that threaten critical infrastructure including obsolescence, human error, accidents, lack of maintenance, simple wear and tear, and space weather and intentional destruction. Critical infrastructure protection (CIP) includes rebuilding or replacing vital systems and services, fortification and insulation, repair, with the increasing use of computers, both physical and cyber infrastructure became more vulnerable.

Most of the physical and cyber infrastructure were owned and operated by the private sector, making federal action limited.

DANGER HITS CLOSE TO HOME

The United States became a target for organizations and individuals that distrusted us, including the World Trade Center attack and the Alfred P. Murrah Federal Building in Oklahoma City.

PRESIDENTIAL COMMISSION ON CRITICAL INFRASTRUCTURE PROTECTION (PCCIP)

Following the Oklahoma City bombing, then President William J. Clinton on June 21, 1995 signed Presidential Decision Directive 39 (PPD 39) *http://www.ojp.usdoj.gov/odp/docs/ppd39.htm*, establishing the Critical Infrastructure Working Group (CIWG), an interagency panel to assess what could be done to minimize or prevent similar events in the future.

In response to the CIWG Report, President Clinton on July 15, 1996 issued Executive Order 13010 http://fas.org/irp/offdocs/eo13010, creating the President's Commission on Critical Infrastructure Protection (PCCIP). The PCCIP report outlined the vulnerabilities of the sectors including the dangers posed by the interdependency among networks.

As a follow up to the Commission report, President Clinton on May 22, 1998 issued Presidential Decision Directive 63 (PPD 63) http://fas.org/irp/offdocs/pdd/pdd-63.htm, which included creation of various new departments within existing federal agencies, among them the National Infrastructure Protection Center (NIPC) within the FBI.

- CHAPTER TWO -

FBI Cleveland Division History

InfraGard began as a pilot program in the FBI's Cleveland Division in 1996. Given the importance of the office to the development and expansion of the program, it is fitting to look at the history of the office to provide the context of the story we tell here. This history was found at the Division's web site on fbi.gov and is used with permission.

The FBI first stationed agents in Cleveland during the earliest days as an organization. By 1914, there was an official Bureau office in the city with a special agent in charge.

By World War I, the Cleveland Division was playing a significant role in the Bureau's national security work, targeting slackers and war opponents under the laws and policies of the day – including prominent anti-war socialists like Charles Ruethenburg, Amos Hitchcock, and Eugene Debs.

Following the 1918 armistice, Special Agent in Charge Charles DeWoody and the agents of the office continued to address national security issues. For example, following a series of failed mail bombings, anarchists attacked a number of political and economic leaders across the country in 1919, setting off bombs in Cleveland, Washington, and other cities.

Although John Dillinger and his gang were out of business by 1935, Cleveland special agents handled many other noted gangster cases. They followed numerous leads in connection with the Barker-Karpis investigation and even welcomed Director Hoover to the office in 1936 when he personally directed the capture of Harry Campbell, an associate of Karpis. The next year, Cleveland agents swore out warrants against Alfred Brady, Clarence Lee Schaffer, and James Dalhover for a large number of robberies and other federal crimes committed in their jurisdiction. The cased eventually led to Bangor, Maine where Brady and Schaffer were killed when firing on FBI agents. Dalhover was captured and eventually convicted of his crimes.

The advent of World War II saw the FBI and the Cleveland Division expand in resources and responsibilities as national security became the top priority. Cleveland personnel provided extensive security checks for local war-related plants, tracked rumors of enemy agents, investigated espionage matters, and kept up wide a wide variety of other criminal matters already of concern. With the onset of the Cold War, the Cleveland Division's national security focus continued as it helped uncover hundreds of ideological agents working for Soviet intelligence.

In the 1950s, the Cleveland Division played a key role in the investigation and eventual prosecution of Communist leaders under the Smith Act, an antisubversion law. In 1956, Joseph Brandt, Martin Chauncey, Frank Hashmall, Anthony Krchmarek, Israel Kwatt, and Lucille Bethancourt were found guilty of violating that Act. Eventually, however, the Supreme Court overturned their convictions, questioning validity of the law.

Major violent crimes – including bank robberies – remained important to Cleveland investigators as well. Significant organized crime leaders in the area were pursued under the Bureau's "Top Hoodlum" program, and the Cleveland Division's Akron Resident Agency played a crucial role in investigating Frank

Lawrence Sprenz, a Cleveland Top Ten Most Wanted fugitive. Sprenz was eventually captured in Laredo, Texas in 1959, seven months after being added to the Top Ten list.

The cultural and political turmoil of the 1960s impacted the Cleveland Division along the rest of the FBI. Cleveland agents investigated radical organizations like the Socialist Workers' Party and violence prone groups like National Knights of the Ku Klux Klan and the Black Nationalist group known as "New Libya." They also arrested the members of a group that supported draft-evasion by forging government papers. On May 7, 1970, the Cleveland Division began investigating the shootings at Kent State University, where four students were killed by Ohio National Guardsmen. Some of the investigations of this era – and Bureau tactics used in them – came under significant criticism following the Watergate scandal, and significant changes were made in FBI policies and practices beginning in the 1970s.

The Cleveland Division's criminal work continued to be successful. In 1969, for example, agents apprehended Top Ten fugitive Jerry Lyn n Young and his accomplice in Akron. They also successfully pursued the killers of United Mine Works official Joseph Yablonski and two members of his family, who were murdered in 1969. The perpetrators were either convicted or pled guilty between 1972 and 1974.

Such work was not without its dangers. On August 9, 1979, Special Agent Johnnie L. Oliver, who had been assigned to Cleveland in 1972, was shot and killed in the city while pursuing fugitive Melvin Bay Guyon, who was wanted for kidnapping, rape and armed robbery. Oliver, who was SWAT team member, and five other agents went to a house where Guyon was believed to be residing. Oliver and another agent went through the front door while the other four agents remained outside. Guyon immediately shot Oliver, who was killed instantly, and then escaped through the front window. On that same day, Guyon was added to the FBI's Ten Most Wanted Fugitives list and was later arrested by FBI agents in Youngstown, Ohio. Guyon was convicted of Oliver's murder and received a life sentence.

BY the 1980s, the FBI had begun to rely heavily on new legislative and investigative tools - primarily the use of undercover agents, Title III wiretap authority, and the Racketeer Influence and Corruption Organization (RICO) Act – to dismantle mob families. In Cleveland, the case called "Operation Busmark" illustrates how important these tools were. In this investigation, the Cleveland Division and the Ohio State Police used undercover agents and wiretaps to build a RICO case that led to the conviction of top mobsters like Angelo Lonardo, Joseph Gallo, Frederick Graewe, and Kevin MacTaggart in the early 1980s on drug-running and other charges. Twenty-five federal and 20 state convictions followed from this case. After being sentenced to life in prison in 1983, Lonardo became a cooperating witness, and even more mid-western mobsters went to jail as a result of his testimony.
In the 1990s, the Cleveland Division joined the FBI in turning its attention to the multiplying connections between domestic crime and international threats. In 1999, as a result of a groundbreaking Cleveland Division investigation, P.Y. Yang – president of a Taiwanese company called Four Pillars Enterprises – and his daughter were convicted of stealing trade secrets from Avery Denison, an Ohio adhesives manufacturing facility. Four Pillars thus became the first foreign company convicted of economic espionage under the Economic Espionage Act of 1996.

In another internationally-based initiative – the pursuit of major drug enterprises – the Cleveland Division began playing a central role in the High Intensity Drug Trafficking Areas program, which brings together federal, state and municipal authorities to target major criminal enterprises trafficking in illegal drugs.

[*https://www.fbi.gov/cleveland/about-us/history*]

- CHAPTER THREE -

The Northern Ohio Chapter -- 1996

In 1997, the President's Commission on Critical Infrastructure Protection (PCCIP) finished its work and it was clear the nation was woefully unprepared to deal with a major cyber attack. A new approach was needed to be taken that combined the strengths of agencies across the U.S. Government as well as innovative outreach to the private sector. Given that cyber intruders can be located anywhere and still reach their victims, this interagency center needed to have global capability. The center needed the legal authorities to be able to obtain records and analyze them of information. Finally, the center needed a response capability.
[Testimony by Ronald L. Dick, FBI, before the Senate Committee on Judiciary, Subcommittee for Technology, Terrorism and Government Information Washington, DC, May 22, 2001, https://www.fbi.gov/news/testimony/gao-review-of-the-NIPC.]

FBI Director Louis Freeh directed that a message be sent from FBI Headquarters to the Special Agents in Charge (SAC) of all 56 FBI field offices to identify and coordinate existing infrastructure expertise inside and outside the Federal Government and provide suggestions on how to best involve the private sector in bilateral information sharing with the FBI in response to the Presidential actions related to critical infrastructure protection.
That same year, during July 1996, the FBI's Computer Investigations and Infrastructure Threat Assessment Center (CITAC) was created to coordinate and program manage investigations involving computer crimes and national security and terrorist cyber threats to the national infrastructure. With the establishment of CITAC, the FBI recognized that the formation of alliances with both the public and private sectors was absolutely necessary to ensure a free flow of critical knowledge, as well as to coordinate responses to attacks, on critical infrastructure components. Kenneth M. Geide was the initial Section Chief of CITAC and John McClurg served as the initial Unit Chief of the Critical Infrastructure Protection Unit (CIPU).

SAC PLAN OF ACTION

The FBI Cleveland SAC at the time was Van Harp. Over his thirty-three year career, Harp would serve the FBI in a variety of roles. The initial eleven years as a Special Agent were dedicated to investigating violations of all federal laws within the FBI's jurisdiction with a focus on violent crime, public corruption, illegal drugs and white-collar crime. The next twenty-two years were spent in positions of increasing leadership and administrative responsibilities for investigative squads, field divisions and FBI Headquarters components. Following his service as SAC Cleveland, his final post was Assistant Director in Charge of the Washington, D.C. Field Division and his service was extended an additional year beyond mandatory retirement due to responsibilities in the FBI's response to the 9/11/01 attack, the anthrax investigation and the Washington, D.C. sniper case.

SAC Harp believed in using the team concept to successfully accomplish tasks and assigned Cleveland's response to Director Freeh's message to a team consisting of Joe Persichini, Assistant Special Agent in Charge (ASAC), Robert Fiatal, Supervisor of the Foreign Counterintelligence/Terrorism/Computer

Crimes Squad and squad members Special Agent (SA) R. Gerald Personen and SA Barry Gummow with support from Intelligence Analyst (IA) Anita Fjeldstad and IA Stan Paulson.

SA Jerry Personen had years of experience investigating Organized Crime and was credited with turning Angelo "Big Ange" Lonardo into one of history's leading mob informants. For two years, the lonely Lonardo called Personen collect daily from a federal penitentiary in Missouri, starting in 1983, with information that helped to convict at least 14 mobsters in Cleveland, New York, Kansas City and elsewhere.

Personen knew how mob families and hackers quietly communicated with each other and suggested the same concepts could be piloted between government and the private sector. He and SA Barry Gummow were specifically authorized by SAC Harp to start reaching out to critical infrastructure CIOs and CEOs in the Greater Cleveland area to have conversations about bilateral information sharing with the FBI via secure communication platforms and meetings. The task was difficult at first because of the fear from some in the private sector that inappropriate information could become public and negatively affect stock prices, consumer buying and image reactions among others.

Over time, SA Personen and SA Gummow, along with the help of the newly created Cyber Squad were able to gain the trust of numerous organization representatives from NASA, FAA, U.S. Attorney's Office, hospitals, banks, academia, accounting firms, utilities, consultants, state and local government who met informally with the FBI to put together a public/private partnership to share information about breaches and ways to protect against hackers. This Cyber Squad was led by Supervisory Special Agent (SSA) Mary Trotman and was staffed by SA Brian Vigneaux, SA David Lyons, SA Charles Sullivan and SA Shane Sims.

INITIAL VOLUNTEERS TO ASSIST THE FBI

MICKEY BAUER volunteered to be the group's first President. She had over twenty-one years of experience working in the financial services industry, in both public and private sectors. During that time she wrote information security policies and standards, initiated and developed incident response programs, and defined security requirements for various platforms. Mickey holds a Bachelor of Arts degree from the University of Cincinnati and a Master of Arts degree from Western Michigan University, and was also a Certified Information Systems Security Professional (CISSP). She would later be elected the Executive Director of the Northern Ohio Chapter of InfraGard and President of the Provisional National Executive Committee in October 1998, the group of Chapters from Indiana and Ohio that helped initially in the transition of InfraGard from Cleveland to FBI Headquarters so all FBI field offices could have their own InfraGard Chapters.

By August 1996, a group of private sector and government individuals had volunteered to meet monthly to assist the FBI in identifying cyber threats and attacks. This group included Mickey Bauer, an experienced financial services industry executive; Dave Strothcamp, a computer expert in healthcare; Charles (Chuck) Pachinger, a Certified Information Systems Security Professional (CISSP); Mike Daugstrup, a senior banking official; Dean Fear and John Nolan, education professionals; and Mike Vangelos, a federal banking official.

The group suggested that it constitute itself as an informal, unincorporated group of individuals who would help the FBI develop partnerships with private sector organizations for bilateral information shar

ing. Dave Strothcamp stated "Initially, there was some level of discomfort among executives when they heard FBI but, because FBI agents took time to explain the agenda, to listen to business people's concerns and show how businesses and the FBI could work together, suspicion turned to cooperation. It's not like the FBI is going to come in and take over your organization. They just have to explain what it is they are trying to do - build a long term relationship with businesses."

NAMING OF THE NEW ORGANIZATION

Although unnamed at first, one of the group's first tasks was to come up with a name for the informal partnership created. FBI and some twenty selected private sector representatives met and brainstormed a number of names according to Edward Napoleon, one of the private sector members. Suggestions included ThisThingofOurs (the literal translation of La Cosa Nostra), CyberSecure, CyberGrd, CyberProduct, CyberDefense, CyberSentinel and CyberScreen among others. SA Personen checked with the appropriate federal government agencies and learned Cyber Guard, CyberWatch, CyberSentry, InfoGuard, CyberShield and CyberSafe were already legally assigned and so unavailable.

Bob Heim, President of the Information Systems Audit and Control Association (ISACA) Chapter, was invited to attend one of the meetings suggested the group try to come up with a name that encompassed infrastructure,
guarding, information, protection and technology. He then recommended InfraGuard which those in attendance liked. Later, as he drove the 22 miles to his home, he regretted that his recommendation did not accomplish his original intent but now he is amazed and proud that the name has lasted 20 years. After the meeting, Dave Strothcamp learned the name InfraGuard was already being used by a software firm and at an October 4, 1996 meeting, suggested that it be spelled and called InfraGard. That name, he added referred to guarding our Nation's information infrastructure. It had the added benefit of not being previously legally assigned, and its unique spelling can be used as a recruitment tool by saying the only thing missing is u (you).
[Cleveland Plain Dealer, 5/19/2010, *http://www.cleveland.com/obituaries/index.ssf/2010/05/r_gerald_personen_nailed_top_m.html*, accessed 8/29/2016.]

FIRST INFRAGARD MISSION STATEMENT

The first mission statement of the new organization was finalized in November 1996:

From left to right: Michael Vangelos, Mike Daugstrup, Mickey Bauer, Dean Fear, Chuck Pachinger, Dave Strothcamp, Jerry Personen

> InfraGard is a cooperative effort in the exchange of information between the business community, academic institutions, the FBI and other government agencies to ensure the protection of our information infrastructure through the referral and dissemination of information regarding illegal intrusions, disruptions and vulnerabilities of the information systems (of Northeast Ohio). The members of InfraGard believe the protection of the information infrastructure is crucial in protecting the integrity and continuity of the institutions and businesses of our respective members, thereby ensuring the health, safety and welfare of the citizens [of Northern Ohio].

Membership

With its core members and alliance with the FBI Cleveland Division, the first InfraGard Chapter welcomed new members. Requirements for these members included agreeing to a Code of Ethics, entering a number of confidentiality agreements and making a Participation Commitment. In committing to these basics regarding sharing confidential information via InfraGard members received several basic services including:

1. Assistance with development of internal protection systems;
2. Provision of a secure source for communicating system intrusion information;
3. Development of a fraud prevention/security awareness program; and
4. Establishment of an Action Committee to solicit supportive legislation and vendor product enhancement.

Given the centrality of the confidential exchange of vulnerability information, a means of secure communication was needed between group members and the FBI. To meet this need, a software solution was needed. The first InfraGard software was created by the AT&T Corporation for the FBI. It used encryption and user authentication features to allow the FBI and member corporations to send and receive secure files and electronic email. If an unauthorized user were to break into a company's computer system, detailed non-disclosure agreements allowed the FBI to analyze the company's computer files and issue warnings to other InfraGard members. This way members learned what clues and technical nuances to look for to prevent a similar intrusion. The software was loaned by the FBI to members.

A less sensitive, more public means of communication was also welcomed. Anita Fjeldstad, an FBI Cleveland Intelligence Analyst, published newsletters for the InfraGard Chapter from November 1997

to November 2000. The newsletters were initiated as a means of communicating with the members of InfraGard on a regular basis. They were intended to be a source of general information to be issued on a monthly basis and include comments, suggestions and submissions from the various committees of InfraGard as well as its members.

The success of the first InfraGard Chapter in organizing itself, was soon noticed. A September 10, 1997 Cleveland Plain Dealer newspaper article indicated the FBI was starting to offer anonymous computer hacking alerts to corporations that agreed to report breaches to the FBI. There was hope by the FBI in Cleveland that private sector organization Chief Executive Officers would change their policies from one of non- reporting to one of sharing with the FBI and anonymously with trusted InfraGard members. It was to their advantage to report computer intrusions and to fulfill a moral responsibility to the computer community colleagues at large.

First InfraGard Officer Elections

In November 1997 the chapter held its first election. There was a decision to have one Chairperson and the rest of the officers to have titles by function. The results named Mickey Bauer as Chairperson; Dave Strothcamp for Administration (organizational support and a point of interfaced for new members); Mike Daugstrup for Influence (an action committee for improvements to software, hardware, regulations, legislation, etc.); Dean Fear for Awareness (informational programs and materials on security concerns); Mike Vangelos for Prevention/Response/Information and practices to prevent or address system intrusions); Charles (Chuck) Pachinger for Communications (electronic communications for the group, continued development of database and website).

EARLY EXPANSION

The initial development of InfraGard was considered a success and the Bureau wanted to expand the pilot program beyond the Cleveland area. In January 1998 SA Personen was authorized to speak with a number of people in Columbus, Ohio interested in forming an InfraGard Chapter. The next month, some Cleveland InfraGard members spoke to the Columbus group. Soon after, the speakers had also met with individuals from Indianapolis, Evansville and Ft. Wayne, Indiana, as word of InfraGard spread across the Midwest.

- CHAPTER FOUR -

The Expansion of InfraGard and the Maturation of the Cleveland Chapter

The development of InfraGard fit well into the evolving FBI response to the threat of cyber crime and cyber attacks on critical infrastructure. In July, 1996, the Bureau had created the Computer Investigations and Infrastructure Threat Assessment Center (CITAC) to coordinate and program manage investigations involving computer crimes and national security and terrorist cyber threats to the national infrastructure. It, though, was focused on organizing FBI responses to such threats. According to Michael Vatis, this response was spurred by 1995 Presidential Decision Directive 39, which charged the Attorney General and other cabinet members with assessing the vulnerability of the nation's critical infrastructure and recommending measures to protect such assets. In response to this assessment, the president created the Presidential Commission on Critical Infrastructure Protection (PCCIP). This Commission reported in October 1997, recommending the creation of a national warning center in the FBI. Its purpose was warn of imminent and ongoing attacks on critical infrastructure components.

In anticipation of presidential action, the Bureau created a National Infrastructure Protection Center (NIPC) at FBI Headquarters on February 26, 1998. It was formally designated as the key component in the national infrastructure protection effort by Presidential Decision Directive 63 (PDD-63), issued in May, 1998 by President Clinton. It established a National Infrastructure Protection Center (NIPC) at FBI Headquarters to detect, prevent and respond to physical and electronic attacks against government facilities, public utilities and private businesses. The NIPC was intended to serve as the federal government's new first line of defense against those who would wage what has been termed "information warfare" - attacks against strategic computer systems by terrorists armed with PCs and modems. For years the nation's defense and intelligence leaders have feared such attacks were possible. But now, with more inexpensive electronics - and a noted increase in intrusions, these same leaders fear that such attacks are probable.

A new approach needed to be taken that combined the strength of federal agencies as well as innovative outreach to the private sector. Given that cyber intruders can be located anywhere and still reach their victims, this interagency center needed to have global capability. The center needed the legal authorities to be able to obtain records and analyze them for information. Finally, the center needed a response capability.

The NIPC could do all of the above and represented a cutting-edge approach to dealing with the difficult problem of computer intrusions. While housed at the FBI, the NIPC was an Interagency Center. It consisted of detailees from the following U.S. government agencies: FBI, Army, Office of the Secretary of Defense, Air Force Office of Special Investigations, Defense Criminal Investigative Service, National Security Agency, General Services Administration, United States Postal Service, Department of Transportation/Federal Aviation Administration, Central Intelligence Agency, Department of Commerce/Critical Infrastructure Assurance Office, and a representative from the Department of Energy, Canada, the United Kingdom and Australia. In addition, the Center had detailees from the Department of State, the National Aeronautics and Space Administration and the U.S. Secret Service as well as state law enforcement officials on a rotating basis. The leadership was drawn from the law enforcement, defense and intelligence communities.

NIPC interagency personnel developed a training program for not only FBI personnel but also for federal, state, local and foreign law enforcement and security personnel. The NIPC training unit had five core courses that concentrate on computer and network investigations.

The NIPC issued a number of warning products that preceded incidents or prevented them entirely by alerting the user community to a new vulnerability or hacker exploit before acts were committed or exploits used on a widespread basis. The Center had particular success in alerting the user community to the presence of Denial of Service tools on the network and has in some cases provided a means to discover the presence of tools on a network.

The NIPC routinely shared information with the public and private sector so as to allow them to better protect themselves. That does not mean information was broadcast across the news media in every instance. While public statements were the best alternative in some cases, in other cases the NIPC had approached victim companies or private agencies privately. In many cases a tiered approach was taken so that information with the appropriate level of detail reached the right audiences. This was particularly important in instances where a company had fallen victim to a well-known vulnerability. Private notification allows the company to repair the breach without publicity. If the NIPC found that despite issuing an advisory, the problem persisted or grew, then that advisory may be reissued.

[Testimony by Ronald L. Dick, FBI, before the Senate Committee on Judiciary, Subcommittee for Technology, Terrorism and Government Information Washington, DC, May 22, 2001].

NIPC AND THE NATIONALIZATION OF INFRAGARD

It was in the midst of these developments that the push to nationalize InfraGard began in earnest. Thus, as SA Personen and Cleveland chapter members began to introduce the idea in the Midwest, FBI Headquarters began to appoint personnel to assist and guide the effort. Michael Vatis, an attorney in the Department of Justice, was appointed Chief of the new FBI NIPC program and Supervisory Special Agent David A. Ford was placed in charge of the nascent national InfraGard program as Acting Unit Chief for the Outreach and Field Support Unit. Ford had entered on duty as special agent in 1992 and worked a variety of criminal investigative matters. In 1997 he was transferred to Headquarters working on several types of cyber investigations. Another key player was new NIPC Section Chief Kenneth Geide who had been instrumental in the FBI's early efforts to address nation-state cyber threats. Geide was known for encouraging the development of intelligence sharing programs with the private sector and the Cleveland Chapter was an obvious model for this effort.

As the first supervisor in charge of national outreach for CIP, the limited efforts of the Cleveland Chapter were most welcome. SSA Ford made numerous trips to Cleveland to visit the first InfraGard Chapter and subsequently traveled to Columbus and Indianapolis, the next chapters to be formed. SSA Ford worked closely with Steven Chabinsky and Michael Woods, attorneys with the FBI Office of General Counsel, to develop membership documents and intelligence sharing protocols for this unique program. He also worked with FBI graphic artists to develop the InfraGard logo. There were several discussions at Head quarters as to whether the FBI should propose changing the InfraGard name, but Headquarters leadership ultimately decided to keep the InfraGard name intact because it was creative and best represented the organization's purpose. A team of consultants from Booz Allen Hamilton provided significant sup

port in the initial rollout of InfraGard and prepared documents and presentations to describe the structure and goals of the organization.

As the national rollout of InfraGard gained momentum, FBI Director Louis Freeh received regular updates about the program and excitement about this new information sharing initiative began to spread to other federal agencies in Washington, DC. In early 1998, SSA Ford briefed Attorney General Janet Reno on the InfraGard initiative and gave numerous presentations throughout the country to generate awareness and support for InfraGard's expansion. At that point, he transferred to the FBI's Atlanta Division Office to head up a new regional computer crime investigative effort and other initiatives and SSA Paula Wendell transferred from FBI San Francisco to FBI Headquarters and became the Unit Chief responsible for the InfraGard Program in August 1998. The effort to nationalize InfraGard was well supported and moving forward rapidly.

THE CLEVELAND CHAPTER MATURES

As it began sharing its experience in early 1998 and settling into a stable organization, the Cleveland Chapter began to consider iconography for its chapter. Mike Daugstrup distributed two proposed logos that had been developed by an FBI Headquarters Special Projects Section- Lab Division sketch artist at the request of SSA David Ford for review in February 1998.

The first of the two logos was preferred, but modified so that the American flag was turned so the stars were on top and the stripes were on the bottom. The rest of the logo was divided into three sectors with symbols representing the government (Capitol dome), private sector/industry (gears) and academia (columns).
The logo was approved as modified and the following regulations were issued later:

> "Use of the InfraGard logo ["seal"] is governed by the FBI Guidelines for use of the InfraGard Service mark which are available on the InfraGard secure website. In general, no business entity (whether a for-profit entity or not-for-profit corporation, sole proprietorship, partnership, educational institution, associa-

SSA David Ford

tion, alliance, etc.) may use the InfraGard name or logo without express written approval of the FBI. Persons who are InfraGard members in good standing may state in writing or otherwise, without further permission, that they are InfraGard members, they are voting affiliates of the InfraGard Members Alliance, and members of their InfraGard Chapter. Persons who are InfraGard members, without further permission, may place on business cards or personal stationary the InfraGard logo with the inclusion of the tag line: "A proud member of". The same logo may include the name of the InfraGard Chapter underneath the graphic. NO PERSON MAY USE THE INFRAGARD LOGO WITHOUT THE TAGLINE. Non-members may not use the InfraGard logo."

Cleveland was showing the way for the progam's expansion in other ways too. On June5, 1998, the Chapter held its General Membership Meeting. Members were congratulated on the Cleveland Chapter being such a successful pilot project and told that FBI Headquarters was taking steps to make InfraGard a national program with all 56 FBI field offices designating InfraGard points of contact. SA Barry Gummow, from the FBI's Cleveland office, a leading expert in forensic computer investigations for the previous nine years, served as the first speaker in the InfraGard Speaker Series on June 5, 1998 and SA Mike Daugstrup briefed the membership on a series of meetings sponsored by Key Bank at which the concept of InfraGard was presented to the "Group of 25" representing the 25 largest banks in America, and the "First Merit Group", representing another 30 very large banks.

THE FORMATION OF A PROVISIONAL NATIONAL EXECUTIVE COMMITTEE

That summer, the push to nationalize InfraGard continued. The FBI held an "InfraGard Seminar" on July 24, 1998, more than 150 people attended from Indiana, Pennsylvania, Illinois, Massachusetts, Virginia, Wisconsin, Michigan and New York, in order to introduce more people to the program. And on August 14, active InfraGard members – the mid-western Chapters that had been created – held a teleconference. The result of this was that leaders from the Cleveland, Columbus and Indianapolis chapters began work on the Non-Disclosure Agreement, the Code of Ethics, the Membership Application and local templates were mentioned.

CLEVELAND (OHIO NORTH CHAPTER)
INITIAL ACCOMPLISHMENTS MENTIONED IN PUBLICATIONS:

- *Prevention/response checklists and guidelines document.*
- *Procedure for influence efforts.*
- *Roll-out of Secret Agent encryption software.*
- *Website design recommendations.*
- *Membership database format.*
- *Preparation of initial chapter start-up kit.*
- *Seminar at a local university.*
- *Developing initiative for a partnership in continuing information security education.*

INFRAGARD CODE OF ETHICS

It is my responsibility to:

- *Promote the protection and advancement of the critical infrastructure of the United States of America.*
- *Cooperate with others in the interchange of knowledge and ideas for mutual protection.*
- *Support the education of members and the general public to enhance their understanding of information security and national information infrastructure issues.*
- *Serve in the interests of InfraGard and the general public in a diligent, loyal, honest manner, and not knowingly be a party to any illegal or improper activities.*
- *Maintain the confidentiality, and prevent the use for competitive advantage at the expense of other members, of information obtained in the course of my involvement of InfraGard, which includes but is not limited to information concerning the business of a fellow member of company, and information identified as proprietary, confidential or sensitive.*
- *Abide by the National and Local Chapter InfraGard Bylaws.*
- *Protect and respect the privacy rights, civil rights, and physical and intellectual rights of others.*

Representatives from the Cleveland, Columbus and Indianapolis chapters worked together with the FBI to finalize the basic documents needed to roll out InfraGard on a nationwide basis. One of the most significant advances was the election of a Provisional National Executive Committee in October, 1998, consisting of six members, two from each of these three chapters. Mickey Bauer and Mike Daugstrup represented Cleveland, Craig Little and Joe Martin Indiana, and Steve Romig and Bill Yang reprsented Columbus. Steve Romig resigned and was replaced by Jeff Schmidt. Later, Charles Pachinger replaced Mike Daugstrup. The purpose of the Provisional National Executive Committee was to act as the national leadership until such time as a National Congress is convened and a formal Executive Board could be elected by the nationwide InfraGard chapter representatives.

FBI PERSONNEL CHANGES

FBI Headquarters personnel, though, continue to change as FBI SSA Brett Hovington was transferred from the Washington, D.C. field office to the NIPC in 1998 and worked for Unit Chief Paula Wendell and NIPC Director Michael Vatis. With assistance from FBI Intelligence Analyst Linda Franklin until her un

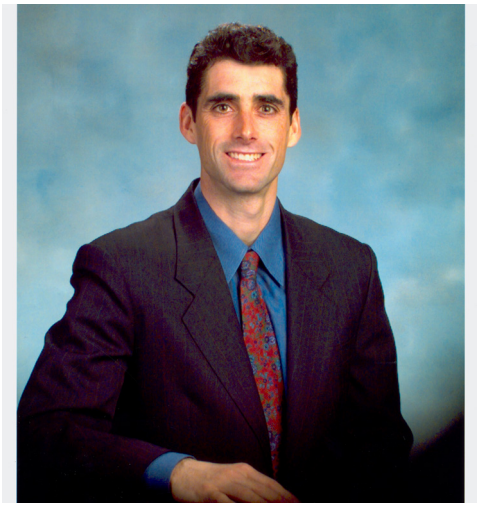
timely death as a result of the D.C. sniper on October 14, 2002, SSA Hovington continued to work with FBI Office of the General Counsel attorney Steve Chabinsky and private sector organization representatives, including Dr. Phyllis Schneck, to translate the Cleveland InfraGard Chapter model into a model that could be used by all 56 FBI field offices.

Another noteworthy change in NIPC personnel was the assignment of FBI Intelligence Analyst Linda Franklin to assist SSA Hovington on all manner of administrative tasks the program generated. On October 14, 2002, though, Ms. Franklin died, one of the ten random, Washington, DC area victims killed during the murderous spree of the D.C. snipers. Her untimely death was a shock to the Bureau and to NIPC. In her honor, a Linda Franklin National Achievement Memorial Award was so named in her

honor as an FBI employee who significantly contributed to the establishment of InfraGard. The award is presented annually to an InfraGard member whose dedication and effort significantly contributes to the advancement of InfraGard and the ideals of the program.

And in September 1999 at the FBI's Cleveland Division Office, FBI Special Agent Dave Lyons replaced SA Personen as the second InfraGard Coordinator.

SSA David Lyons



NIPC Chief Michael Vatis

KEY FBI PERSONNEL

AD Ronald Dick

SSA Jerry Personen

Cleveland SAC Van Harp

- CHAPTER FIVE -

InfraGard and Louisiana State University - 1999

By the start of 1999, Chapter membership meetings were taking place quarterly and the Cleveland Chapter's leadership structure was stable, consisting of an executive director, a membership director and a finance director. In addition, there were to be four general directors and elections were scheduled to occur in May of that year. The chapter also embarked on a training initiative by contacting local colleges and universities to assess training needs and develop courses or seminars on a range of topics and in a variety of formats.

At the Cleveland Field Office, SA Dave Lyons was sent to FBI HQ on a temporary assignment to assist SSA Dave Ford with the roll out of the national InfraGard program. SSA Ford agreed to conduct the first national conference to assist potential members from 16 different cities who had shown interest in initiating their own InfraGard chapters. The meeting was held in Cleveland over March 16 and 17, 1999. Additional conferences were held in November 1999 in Pittsburgh, San Francisco and Milwaukee, led by Dave Strothcamp and Gary Sheehan from the Cleveland chapter membership and FBI Special Agent InfraGard Coordinator Dave Lyons.

The InfraGard model was becoming so popular that SA Dave Lyons and Dave Strothcamp even went to Japan to explain the InfraGard concept that year. Nor was InfraGard the only responsibility SA Lyons had. During this time he was also investigating the theft of Alzheimer's research data and the theft of adhesive technology from the Cleveland area. These cases were persued under a new Economic Espionage statute that had been passed only three years earlier.

INFRAGARD WEBSITE/PORTAL

Another milestone in the evolution of InfraGard was the institution of its secure website, a key feature for the program in that it provided members a secure way to communicate with one another and the FBI. Access to the website was provided to those InfraGard members who had executed the Secure Access Agreement that had been developed earlier that year. FBI Headquarters worked to develop additional content for the site in order to improve its utility for InfraGard members. Complementing the website was the roll out of the latest version of AT&T Secret Agent encryption software. The software secured the exchange of information within the InfraGard Alert Network. But members wanted something that would blend the two together and make more of an on-line community for all chapters and their members. FBI Intelligence Analyst Linda Franklin raised similar concerns, noting the need for a Help Desk and a secure internet portal in order for the expanding InfraGard membership to communicate effectively.

The FBI was concurrently working on a secure means for law enforcement officers to exchange information over the Internet. It was called Law Enforcement On-Line or LEO. It is an online (real time), controlled-access communications and information sharing data repository. It provided a focal point for electronic Sensitive but Unclassified (SBU) communication and information sharing between federal, state,

local and tribal law enforcement agencies.

This system was managed by Louisiana State University IT contractors, who maintained the infrastructure of LEO and the LEO Support Center. On the FBI's end of the project was Special Agent Gary Gardner, who managed LEO and the LSU contract within the National Infrastructure Protection Center (NIPC). IA Franklin and SSA Hovington approached SA Gardner for assistance in contacting Louisiana State University [LSU] about helping out the InfraGard program. SA Gardner had LSU draft a contract, modeled on the existing LEO contract. The three presented it to their leadership and recommended its approval. It was quickly approved and LSU became the subcontractor for the InfraGard web portal too.

Under the contract, LSU agreed to provide InfraGard with a mechanism for law enforcement entities and private sector members to share sensitive data internally and externally with critical infrastructure personnel. The system also provided an internet accessible focal point for electronic SBU communications and information sharing for InfraGard members.

THE ALERT NETWORK

Perhaps the most important aspect of this new web portal was the "Alert Network." It was designed to provide each InfraGard member with a mechanism to voluntarily notify the FBI in the event of a physical or cyber attack. When a member determined that a report was appropriate, the member used encryption technology furnished by the NIPC to send descriptions of the incident to the NIPC. Minimally, the reports included:

- A "sanitized" description of the incident provided relevant information but did not identify the victim member. At the member's option, this description was furnished by the NIPC to (1) other InfraGard members who have signed a non-disclosure agreement, and/or (2) to the public so they may take action to protect their own systems:
- A detailed description of the incident gave the NIPC information about the victim's identity and enough background to conduct an in-depth analysis of the threat. The FBI used the detailed report to determine if a criminal or national security investigation is warranted.

The NIPC also took information supplied by the members of InfraGard, the Intelligence Community, and criminal investigative sources to produce periodic threat reports for InfraGard members.

INFRAGARD SECURE WEBSITE

Ultimately, the secure website that LSU developed for InfraGard provided members with information about recent intrusions, research related to infrastructure protection, and the capability to communicate securely with other members. The website had the following features:

- What's New"--Real-time information about infrastructure protection;
- Sector News"-Critical Infrastructure related links, recent news articles and press releases;

- Chapter News Internal links for each Chapter to post chapter-specific information;
- Discussion Groups A secure, integrated electronic discussion group capability
- Related Links External links to NIPC Web Page and additional infrastructure protection resources

- CHAPTER SIX -

The Continued Growth of InfraGard

2001-2002 National Executive Committee Members:

Bill Yang, Columbus, Chair
Dr. Phyllis Schneck, Atlanta, Co-Chair
James Joyce, St. Louis, Secretary
Jeff Schmidt, Columbus, Treasurer
Dave Strothcamp, Cleveland
Shantel Wilkins.

2002-2003 National Executive Committee Members

Dr. Phyllis Schneck, Atlanta, Chair
James Joyce, St. Louis, Co-Chair
Bryan King, Pittsburgh, Secretary
Jeff Schmidt, Columbus, Treasurer
James LeGrand, Virginia
Rob Schmidt, Chicago.

The expansion of InfraGard across the nation continued as the world prepared for the Twenty-First Century. In January, 2000, the Provisional National Executive Committee of InfraGard traveled to the Capitol to assist with the second national rollout conference, where another 34 FBI field offices were introduced to the concept of InfraGard. The NIPC had been supporting the expansion of the new InfraGard chapters in cities across the United States. Chapter initiation conferences were planned in Los Angeles, Little Rock and Honolulu.

The NIPC also produced a one-hour program that was broadcast live across LawTV, a law enforcement satellite-cable station. In the program, Steve Chabinsky, from the FBI's Office of General Counsel discussed the legal ramifications of InfraGard to the law enforcement communities. The NIPC was also in the planning stages for InfraGard National, the first national workshop/conference for leaders from the non-FBI part of InfraGard to come together to discuss the direction of the organization and chart out the future steps needed to ensure the protection of critical infrastructures.

Dave Strothcamp, of the Cleveland Chapter, returned to Japan for a second presentation in 2000. There he noted that through InfraGard, he had seen the significant progress that can occur when business and government each shares talents, specialized technical knowledge and work experiences to develop cost effective educational programs that will enhance the security of our national computer infrastructure. He noted that sharing based on trust and mutual respect was what makes the InfraGard Program unique and promoted strong partnerships between law enforcement, government and organizations within the private business sector.

Membership continued to grow through August 2000 as the FBI's offices in Richmond, Va., Charlotte,

EXCERPTS FROM ANNUAL REPORT TO MEMBERSHIP
(July 1, 2001-June 30, 2002)

The past year has brought a renewed sense of urgency to the InfraGard initiative. The energy of our leaders, members and affiliated partners, coupled with tragedy in our Nation, has brought industry and government together in an unprecedented force to enhance and protect critical infrastructures. InfraGard served as the unique liaison between the private sector and the U.S. Intelligence Community. Partnered with the NIPC to ensure interaction with all government agencies, InfraGard provided the connection between companies, academic institutions, government and law enforcement by1) leveraging the existing InfraGard trust network of almost 5,000 members, 2) leveraging relationships already formed by other agencies, partnerships and functioning ISACs, and 3) building connections from intelligence agencies and ISAC-level information to all critical infrastructure operators, independent of size or stature.

Following September 11, 2001, the National Infrastructure Protection Center expanded its efforts to include physical as well as cyber threats to critical infrastructure.

The InfraGard National Executive Board (INEB) was responsible and accountable for continuing to build the InfraGard trust network based on the vision and direction of members. The INEB used guidance from our constituents in refining the information sharing model to most efficiently leverage the existing successes of InfraGard and other organizations while building relationships and connections where they are currently absent. Time was of the essence, as critical infrastructure protection was key to protecting our Nation. We sought aggressive growth in information sharing over all of our critical infrastructures utilizing the InfraGard partnership and, with that, we also sought improvement of the communications processes among our members and INEB to facilitate positive change as an organization that serves its members.

Key to the success of the InfraGard partnership was local Chapter participation, awareness and inclusion. To expedite accurate and efficient communications between local Chapters, the INEB divided the Nation into six distinct regions and appointed six InfraGard members to be known as Regional INEB liaisons. At the 2002 Congress, regional groups will consider membership structures (do we need background checks); incorporation, bylaws, and private funding; partnerships, growth, and future directions; and information sharing (leveraging local Chapter expertise nationally, and development of a speakers bureau).

BYLAWS:

When the InfraGard Bylaws were initially created in 1996, they were designed to enable a budding organization to take shape. The InfraGard organization is now a functioning partnership that requires more robust bylaws. Hence, the INEB has spearheaded, with a team of attorneys, some changes designed to enable InfraGard to grow in many new directions for years to come.

The biggest issue that may arise is the clarification of the point of executive authority in the organization. Legally speaking, InfraGard's authority comes from the central, National organization, although the National organization has tried to maximize the distribution of authority down to the local chapter level. That distributed authority is checked and balanced by the express authority and power of the local chapters to change the leadership on the InfraGard National Executive Board. The local chapters are the core of the InfraGard partnership, and, therefore, most authority for operational concerns will be delegated to the local chapter level. The bylaws presented at the Niagara Falls Congress failed to pass.
InfraGard strived to be the unique and trusted connection for business to government and law enforcement. If other organizations consistently have information ahead of InfraGard, this defeated the purpose and mission – even though the InfraGard information may be better investigated or may be of higher integrity given its FBI origins.

METRICS:

In previous years, InfraGard measured the progress of individual chapters, as well as the overall organization, by the number of members and member companies. As InfraGard evolves to a functional and more mature organization, member quantity alone is no longer an accurate measure of success. The INEB proposed the following measures be explored to form a more accurate quality assurance and growth measurement formula for InfraGard for the near term:

Information Sharing – Information sent from local chapters to the NIPC; Information received from the NIPC to local chapters; Accuracy of information: Speed of receipt of information; and Cost savings to

any party upon receipt or distribution of information;

Membership – Number of members; Number of member companies; Member composition (e.g. members representing the nine critical infrastructures); Member company composition (e.g. good spectrum of size, type of company); Member participation in local chapter; Member participation in regional discussions/activities; Member participation in national initiative; Composition of local steering board; and Frequency of elections and terms of elected office;

Chapter Outreach – Number of chapter meetings; Types of meetings; Membership retention (helps to demonstrate value added that brings people back).

ORGANIZATIONAL OUTREACH:

InfraGard at its core is a network of trust. Traditional marketing efforts are needed moving forward, yet trust must always be the foundation of InfraGard. Therefore, InfraGard marketing efforts need to be focused and directed toward adding value to a target audience while always upholding the integrity of InfraGard. Expansion of the InfraGard trust network has occurred in three key ways:

1. Strategic relationships with industry, government and academia;
2. Local interactions, programs, education and awareness;
3. Strategic Interest Groups (SIGs); e.g. the first SIG, the new InfraGard Manufacturing Industry Association (IMIA).

MOVING FORWARD:

InfraGard had many success this first official year and must maintain this momentum. As it leverages the foundations set, InfraGard must focus now, more than ever, on using the trust network to increase frequency, speed and accuracy of information exchange. This means working closely with other government agencies and building channels for communication where they do not already exist. InfraGard must concentrate on bringing value to members and on continuing to build the trust network from the "grass roots" to the highest levels of government. InfraGard will also be working closely with the NIPC and other agencies to forge international relationships, as information sharing must be global if it is to be fully implemented and effective in the future.

On a more tactical level, to meet the needs of the InfraGard partnership, the organization and INEB must establish more refined processes to expedite administrative tasks such as application, member tracking and information distribution. InfraGard needs a faster membership acquisition cycle, a secure form of electronic communication, and augmented and more efficient channels and processes of communication between Federal, State and local governments.

The vision of InfraGard in the Strategic Plan was to become a highly-regarded, definitive source of information dedicated to the protection of critical national infrastructures, and to be the designated private sector group to partner with the government to focus on the following challenges that can only be met via true partnership and information sharing. Strong alliances with government agencies coupled with leadership, participation and education at the local and National level will truly render InfraGard the trusted partnership for protection. It is our responsibility, as an organization and as a Nation, to build this network and to sustain this partnership.

N.C. and Jacksonville, Florida, partnered with local businesses to form InfraGard chapters. By November 2000 it was announced that the national rollout was nearly complete: 54 out of 56 cities had formed local InfraGard chapters over the previous two years. The flexibility of chapters to develop their own unique flavor was certainly an asset and enabled them to be most responsive to their members.

All of this expansion culminated on January 6, 2001, when the FBI and NIPC introduced the National InfraGard Program to the public. The national program, like its more local components, would provide four basic services to its members:

1. an intrusion alert network using encrypted email,
2. a secure website for communication about suspicious activity or intrusions,
3. local chapter activities, and
4. a help desk for questions.

The critical component of InfraGard, the press release stated, was:

> "the ability of industry to provide information on intrusions to the local FBI Field Office using secure communications in both a "sanitized" and detailed format. The local FBI Field Offices can, if appropriate, use the detailed version to initiate an investigation; while the NIPC at FBI Headquarters can analyze the information to determine if the intrusion is a broader attack on numerous sites. The NIPC can simultaneously use the sanitized version to inform other members of the intrusion without compromising the confidentiality of the reporting company. In addition, the secure website contains a variety of analytic and warning products that can be made available to the InfraGard community."
>
> [FBI National Press Release, 1/6/2001, *https://www.fbi.gov/news/pressrel/press-releases/the-fbi-and-the-national-infrastructure-protection-center-publically-introduce-the-national-infragard-program*, accessed 7/7/2016.]

LOCAL CHAPTER ACTIVITIES

The national organization did not merge the local chapters. Instead, each InfraGard chapter was to develop a specialized program that would address the unique needs of its local membership. Representatives from the local FBI Field Office would assist InfraGard members in identifying their infrastructure concerns and needs.

The following list suggests some of the activities that local chapters might offer:

- Seminars and conferences in infrastructure protection,
- Regular chapter meetings where members present discussion topics,
- Infrastructure protection education and training,
- A local newsletter,
- A contingency plan for using alternative systems in the event of a successful

large scale attack on the information infrastructure, and
- A cyber awareness campaign for members and non-members.

INFRAGARD NATIONAL EXECUTIVE BOARD

As part of the creation the national program, the InfraGard National Executive Board (INEB) was formed in 2001 to assist with the formation of governance measures that were implemented on a national basis. Members of the INEB were to possess a number of attributes, including: previous board experience (corporate, academic or non-profit); leadership and management experience; government and corporate relationships; negotiation experience, superior organizational skills; excellent time management/efficiency; media/public relations experience; effective public speaking skills, writing and editing skills; media training; and a trusted nationwide reputation.

Their responsibilities included communicating with InfraGard members and chapters nationwide, working directly with government and private sector leaders, negotiating benefits for InfraGard members and provide for the group's overall organization, strategic planning, and implementation. They were the new organization's management and would represent InfraGard nationally to its membership, the federal government, and the national press. They were also responsible for project management and execution.

BILL YANG, a senior system and network specialist who had been involved in fostering cooperation and trust between law enforcement, computer, network, and IT professionals for many years and was the first to volunteer to be a member of the Provisional National Executive Committee and became the first Chair of the InfraGard National Executive Board. He held the position from 2001-2002. Yang provided technical and scientific computing support to the higher education and research communities at five universities in Northeast Ohio.

The following year, 2003, as Bill's term as committee chair was coming to an end, Dr. Schneck became Co-Chair of the InfraGard Executive Board from 2001-2002 and was then elected Chair in 2003. Earlier, Dr. Schneck had been President of InfraGard Atlanta where she suggested that the Chapter should be named InfraGard Atlanta so that people could find it more easily in the telephone book; she noted that there were hundreds of organizations whose names started with Atlanta. Due to her professional work and effort with InfraGard Atlanta, Mr. Greg Rattray from the White House National Security Council Office of Cybersecurity pressed her to become involved in helping to expand InfraGard from the original Cleveland Chapter to all 56 FBI Field Offices and to enhance bi-directional information sharing and communication.

FIRST INFRAGARD NATIONAL CONGRESS

With a national leadership, the new umbrella organization held its first National Congress in San Diego, CA June 12-14, 2001. The conclave provided an excellent forum for NIPC senior managers and InfraGard members to exchange ideas.

The InfraGard National Executive Board's first annual report to its members captured some of this fervor.

SECOND INFRAGARD NATIONAL CONGRESS

A Second InfraGard National Congress was held in Niagara Falls, NY June 10-13, 2002. Private industry representatives from 65 local InfraGard Chapters and the FBI InfraGard Coordinators from the 56 FBI Field Offices attended. Highlights of the meeting included keynote speeches by Ronald L. Dick, Director of the NIPC, and Richard A. Clarke, Special Advisor to the President for Cyberspace Security. Also, there was a public ceremony as the NIPC/FBI, the U.S. Small Business Administration (SBA), and the National Institute of Standards and Technology (NIST) signed an interagency agreement to provide information technology security for small businesses. Clearly the plan to nationalize the Cleveland Chapter's efforts had proven more than successful.

- CHAPTER SEVEN -

The InfraGard National Members Alliance [INMA] and the InfraGard Members Alliances [IMAs]

With much organizational work completed by its national board, a certificate of incorporation for InfraGard, Inc., was filed with the State of Delaware on April 7, 2003 in the Office of the Recorder of New Castle County. The Third InfraGard National Congress was held that spring in Washington, D.C., from June 23-25, 2003. And, on April 17, 2003, Dr. Schneck became the Chair of InfraGard, Inc. She would then serve as the founding chair and president of the InfraGard National Members Alliance in 2004, when the Executive Board had finished building the National Alliance. She was responsible for the strategic growth and vision of the private sector side of InfraGard, often representing InfraGard in the creation of national policy.

Dr. Schneck said her major accomplishments were evolving the organization from an informal collection of chapters to an official nationally-run organization that enabled rapid, consistent growth while preserving the local culture of the chapters and interactions between private sector and government. There was a formalizing of the roles of the private sector and FBI/government leadership, and a partnership with the "new" (at the time) Department of Homeland Security (DHS). Schneck also introduced the "Chapter-in-a-box" - a product of her InfraGard Presidency and the great team in InfraGard Atlanta that helped many other chapters quickly organize and solve logistical problems easily to get right to real work. Finally, Schneck focused on Chapter Presidents from whom, she said, the culture and leadership emanated.

As of 2016, Dr. Schneck currently serves as the Deputy Under Secretary for Cybersecurity and Communications for the National Protection and Programs Directorate (NPPD). She is the chief cybersecurity official for the Department of Homeland Security (DHS) and supports its mission of strengthening the security and resilience of the nation's critical infrastructure. Dr. Schneck received her Ph.D. in Computer Science from Georgia Tech University, and her Bachelors and Masters Degrees in Science from Johns Hopkins University.

At this time, the National Infrastructure Protection Center was transferred to the Department of Homeland Security in 2003. The FBI, though, retained its role with InfraGard as an FBI Program in the Cyber Division as it worked with DHS in support of the new Department's critical infrastructure protection activities. The Cyber Division also worked to further develop InfraGard's ability to support the FBI's investigative mission, especially as it pertained to counterterrorism and cyber-crimes and so the FBI asked InfraGard to consider CIT as more than simply cyber related matters. Regardless, these Bureau changes had no impact on the move to create the National Alliance or on the work of the local chapters. Each was well established and developing in a healthy manner. To ensure this, the Bureau and the newly formed INMA established their first Memorandum of Understanding (MOU), executing it in August, 2004. Soon, the Department of Homeland Security sought a similar agreement.

That same year, the INMA Board voted to select Michael Hershman as Chair of the first Advisory Board and formed its first Regional Task Forces across the country. As to the administrative offices of INMA, with a structure and operating agreements in place, they established an official address 974 Breckenridge Lane #167, Louisville, KY 40207.

INFRAGARD CORPORATE GOVERNANCE LEGAL ISSUES

Several issues arose between the INMA and local InfraGard Chapters, most of which had no standing as legal entities—they had formed on an informal basis and their incorporation into information sharing with each other and the Bureau was equally informal at first. Such chapters were even unable to open a checking account for local operations because of this lack of legal basis. In addition, they had no formal, legal means of affecting national policy or oversight over the InfraGard National Executive Board (INEB). Nor could the INEB affect the governance of such local chapters or negotiate on behalf of the InfraGard Program with them. This needed to change.

It was in this vacuum that the InfraGard National Members Alliance (INMA) and InfraGard Members Alliance (IMA) Corporate Governance structure was conceived. The work on this was primarily done by Rob Schmidt, Jeff Schmidt, Phyllis Schneck and Steve Chabinsky of the FBI Office of General Counsel. Mark McCarty, the INMA attorney, was also instrumental.

As they tackled the problem of creating a formal standing for local chapters, several issues quickly arose. Primary among them was the question of what form should the INMA/IMA structure take to facilitate the Program's interests/success? Options proposed included:

1. Letting the IMAs keep their geographically diverse and unique infrastructure protection concerns intact.
2. Letting the IMAs govern their own organizations.
3. Letting the IMAs have legal standing (with respect to the INMA) to elect national representation.
4. Letting the IMAs benefit from the economies of scale that a "National Organization" might provide by negotiation with third parties.
5. Providing consistency and easy accessibility for the IMAs (through the INMA) with respect to the policy/goals of the FBI; and
6. Allowing the INMA oversight over IMA corporate operations to ensure they are consistent with the FBI's objectives.
7. Correct the course of errant IMAs (through the INMA) should that course veer from the FBI's policies/goals.

The INMA/IMA structure:

1. Allowed the INMA to license the use of the name "InfraGard" from the FBI (through a Trademark License Agreement). The FBI can pull this license if the INMA is not in line with the FBI policy/goals of the InfraGard Program.
2. Allowed the IMAs to license the use of the name "InfraGard" from the INMA (through a Sub-license Agreement). The INMA can pull this license, should the FBI so desire, if the IMA is not in line with FBI policy/goals.
3. The IMAs also executed a "Voting Member Agreement" with the INMA. This agreement gave the IMAs a legal right to vote on the Directors of the INMA. In return, it acknowledged the IMA must remain in "good standing" with INMA policies/goals.

Benefits of the INMA/IMA Structure from the FBI Perspective:

1. The structure helped protect the FBI's intellectual property (the Service Mark "InfraGard");
2. It established a consistent operational structure for all of the InfraGard Chapters;
3. It provided an "arm's length" relationship that helps protect the FBI from the sometimes unpredictable behavior of IMAs or individual InfraGard members;
4. It relieved the burden on the FBI to manage and administer 80+ private sector groups (all with different goals and objectives); and
5. The flexibility of the structure allowed the FBI to task the organizational components of the InfraGard Program with a variety of potential deliverables.

Benefits of the INMA/IMA Structure from the the INMA's Perspective

1. Prior to the conversion the "INEB" (InfraGard National Executive Board) was a stand-alone entity and was not legally responsible to the "Chapters." The conversion placed a legal obligation and fiduciary duty on the INMA Board and Officers that did not previously exist;
2. The structure also created an obligation on the IMAs' part. The IMAs are obligated to a set of consistent national bylaws and policies;
3. The creation of the INMA as a 501(c)(3) allowed it to raise funds as a non-profit;
4. The structure allowed the INMA to share funds with the IMAs uniformly across the country (in the event the IMA received "use at will" funds from a third party);
5. The structure created a uniform corporate structure that allowed the INMA to negotiate and provide products and services to the IMAs at a substantially reduced cost. (Examples of this are: the availability of Directors and Officers Liability Insurance, the "blanket" 501(c)(3) exemption status from the IRS, and any additional services the IMAs find useful.); and,
6. The uniform corporate structure highlighted that the INMA and IMAs were not FBI controlled entities. This "arm's length" relationship was necessary for a variety of reasons (negotiating with additional government agencies was the best example). Understanding that an "InfraGard Chapter" still has three vital components: an IMA, a group of InfraGard members, and an FBI Field Office.

Benefits of the INMA/IMA Structure from the IMAs' Perspective:

1. The structure guaranteed each IMA a legal right to vote in the affairs of the INMA;
2. The structure created a responsibility on each IMA to adhere to a consistent

set of operational standards (bylaws and national policy);
3. The structure allowed the IMAs to raise funds as non-profits;
4. In the event funds were raised, the structure allowed the IMAs to maintain their own treasuries, separate and apart from the INMA. (The ONLY act that can move funds from an IMA or InfraGard member to the INMA was a national vote);
5. The structure allowed Officers of the IMAs to benefit from the availability of D & O insurance at a substantially reduced cost; and,
6. The structure established the IMA as separate and distinct from the FBI for the purposes of engaging additional local federal agencies and businesses.

The new bylaws were approved during the 2004 Annual Congress that was held in Washington, DC. Subsequently, the INMA Secretary Sheri Donahue provided each IMA with a statement about the status of its IMA Conversion Status and Checklist to provide:

1. Proof of Incorporation and/or name change to conform with the IMA naming convention;
2. Proof of 501(c) (3) status;
3. The Voting Membership Agreement with the INMA;
4. The Sub-License Agreement;
5. Verification the IMA has evaluated its bylaws to ensure they do not conflict with the INMA's bylaws; and,
6. The name of a Membership Coordinator who has executed a Non-Disclosure Agreement (NDA) with the FBI.

The official deadline for creating the IMAs was June 17, 2005 and 68 of 84 IMA Conversions took place on a timely basis.

THE CERTIFICATE OF INCORPORATION FOR INFRAGARD, INC.

On June 29, 2004, the Board of Directors of InfraGard, Inc. adopted a resolution setting forth proposed amendments to InfraGard's Certificate of Incorporation, declaring said amendments to be advisable and submitting the proposed amendments to the local chapters of the Corporation for their consideration and approval, such proposed amendments being legal in nature including the name of the corporation shall be InfraGard National Members Alliance, Inc.

The proposed amendments were duly adopted by a majority vote of the local chapters and the certificate was signed by Sheri Donahue, Secretary of InfraGard, Inc., on July 20, 2004. The old InfraGard National Executive Board will become the Board of Directors of the InfraGard National Members Alliance. Local Chapters will become InfraGard (locality) Members Alliances. The term "Local Chapter" will be defined as: An IMA, an FBI Field Office, and a group of InfraGard members who are affiliated locally by virtue of "voting rights" in an IMA. The IMAs will have Executive Committees that would administer the program locally. In addition, the IMAs will be the legal members of the INMA.

On 12/14/2004 the FBI ran a news story saying that the essence of the partnership was information and intelligence sharing. FBI agents assigned to each Chapter bring meaningful news and information to the

table: threat alerts and warnings, vulnerabilities, investigative updates, overall threat assess

ments, case studies, and more. Private sector partners – who own and operate some 85% of the nation's critical infrastructure – share expertise, strategies, and most important, leads and information that help track down criminals and terrorists.

The story shared a sampling of what local Chapters were doing to protect critical infrastructure:

> • The Philadelphia Chapter had developed the Cyber Incident Detection and Data Analysis Center project which created an automated cyber-attack early warning system to centralize information online threats from participating organizations nationwide.
> • The Las Vegas Chapter helped the FBI capture a criminal who used his employer's computer system to embezzle more than $150,000.
> • The Los Angeles Chapter participated in a two-day, nationwide simulated terrorist attack training exercise with law enforcement and first responders.
> • The San Francisco Chapter trained FBI agents to identify and stop sophiscated programs that hackers use to infiltrate computers.
> • The Vermont Chapter offered free classes to teach local residents how to protect themselves from online threats.
>
> *[https://www.fbi.gov/news/stories/2004/december/infragard_121404*, accessed 7/72016].]

- CHAPTER EIGHT -

Highlights by Year, 2005-2016

2005-2006

In the past year all 'chapters' were incorporated and obtained 501(c) (3) status to become IMAs. That year, the Board passed an amendment to change seven (7) elected board members to be six (6) elected and three (3) appointed board members and the membership, by resolution approved other changes. The most significant was that "one appointed Board position is filled by an elected member with one year left on the member's term. The Board hereby waives its right to appoint said member and will reestablish the appropriate weighting of the Board in 2006…The two directors getting the most votes shall occupy the three year terms."

- InfraGard continued to cooperate closely with the newly created Department of Homeland Security. In the 2005/2006, period DHS hired 68 Protective Service Advisors and they will be oriented about InfraGard.
- IRS confirmed 501 (c) (3) status for INMA.
- Per FBI UC Don Good, each FBI Region will have a Regional IGC assigned in November.
- Initial Advisory Board members, in addition to Chair Michael Hershman, are Courtney Bank, Mark Codd, Jack Johnson and Greg Lebedov.
- INMA engaged a Public Relations firm GCI.
- Jeff Schmidt bought rights for InfraGard.org, InfraGard.net, and InfraGard.Com.
- 2005 was the first year INMA specifically funded by the FBI.
- A contract was signed with Cintas, Inc. in Cincinnati to provide shirts with InfraGard logos.
- Mark McCarty named INMA General Counsel.
- Greg Ratrey and John Clerici named to Advisory Board.
- At the August Congress, two SIGs were recognized: Chemical and AgGard.

2006-2007

During the 2006/2007 period, the ESP Group, LLC, web portal was introduced to INMA members at the yearly congress. The ESP Group, LLC was founded in 2000 as a commercial company dedicated to providing secure collaboration portals to Government and commercial clients.

Through a partnership with the ESP Group, all InfraGard members were provided an opportunity to join its CyberCop Portal at no cost. CyberCop was an SSL-based secure communications environment, developed by ESP Group under DARPA, the Defense Advanced Research Projects Agency that would allow InfraGard members to easily and securely communicate with each other, share documents and receive communications from the INMA.

The CyberCop mission was to provide a highly secure web-based environment to promote and facilitate the sharing of sensitive but unclassified information among law enforcement, security, intelligence, private sector and first responder professionals. Its purpose was to serve and strengthen a cohesive network of participants from all levels of government (international, federal, state and local), academia and industry, regardless of departmental affiliation and jurisdictional boundaries.

CyberCop was committed to providing a safe and secure environment where ideas can be freely exchanged to aid individual efforts and foster cooperative efforts in the fight against crime and terrorism and the protection of the security of our homeland. Because of the success of the CyberCop Portal and the ease of use of the collaboration tools, the InfraGard National Members Alliance created a compartmented "Community" established for InfraGard members ONLY. This new compartment will allow information to be shared within the InfraGard community and will also enable the InfraGard members to collaborate with the other 10,000 CyberCop participants if appropriate.

CyberCop provided many advantages, including:

- secure messaging including attachments to be passed among portal users;
- locator feature that gave contact information for the users in your portal;
- online briefings allow for online presentations;
- public and private library categories allow for easy document sharing;
- a calendar for access to individual event listings; ongoing threaded discussions between selected groups of users;
- create customized surveys to pulse the user community about areas of interest;
- allow for customizable groups, similar to address books, to be used when giving access throughout your portal;
- webports (access controlled web pages inside the portal);
- the TaskTrac tool, which could be used to create tasks, assign resources and keep track of task details; and an
- alert tool so select users can send messages to alert lists. Users that are part of an alert list can customize the way they receive alert information which can include any text-enabled device (phone, pager, PDA, email, etc.).

CyberCop had been endorsed by DHS and would complement the earlier VPN-based system created for the Cleveland InfraGard chapter, which the FBI would continue to operate its. All involved in the adoption of CyberCop fully supported membership efforts to provide additional ways to enhance communication.

Other highlights of the years 2006/2007 included:

- Sheri Donahue and Rob Schmidt drafted and distributed the President's Handbook at Congress.
- INMA voted to participate in the iKeepSafe.org Coalition.
- A new publication titled Gardian was introduced.
- Government Emergency Telecommunications Service (GETS) and Wireless Priority Service (WPS) access was introduced as an IMA member benefit.
- The DHS Daily Report was now being made available to InfraGard members.
- Dr. Schneck, Dr. Kiernan and FBI SSA Chris Dowd met at the British Em-

basy to introduce the InfraGard concept.

- INMA became a partner with the DARE [Drug Abuse Resistance Education] program.

2007-2008

- INMA contracted with Norwich University to obtain services of a part time Managing Director to include an office for INMA.
- INMA mailing address changed from Kentucky to 2425 Wilson Boulevard, Suite 240, Arlington, VA 22201-3326.
- INMA ended relationship with PR firm GCI. To be replaced with monthly Chairman's Corner publication.

The FBI received questions regarding a February 8, 2008 article published online at www.progressive.org, titled "Exclusive! The FBI Deputizes Business." The article was wildly inaccurate and the author went so far as to claim that InfraGard members had been given extraordinary powers to shoot to kill. [http://www.progressive.org/news/2008/03/6052/fbi-deputizes-business, accessed 7/7/2016.]

FBI Cyber Division Deputy Assistant Director Shawn Henry issued the following response on February 15, 2008:

> "In short, the article's claims are patently false. For the record, the FBI has not deputized InfraGard, its members, businesses, or anything else in the program. The title, however catchy, is a complete fabrication. Moreover, InfraGard members have no extraordinary powers and have no greater right to "shoot to kill" than other civilians. The FBI encourages – and all Americans to report crime and suspected terrorist activity to the appropriate authorities."
>
> "Unfortunately, the author of the Progressive article even refused to identify when or where the claimed 'small meeting' occurred in which issues of martial law were discussed. If we get that information, the FBI will certainly follow up and clarify any possible misunderstandings."
>
> "The FBI strongly supports the InfraGard program and recognizes that the protection of our critical infrastructure – most of which is owned and operated by the private sector – requires that we develop productive relationships with and amongst industry. It is certainly the case that some of these discussions require confidentiality, and the InfraGard program provides a valuable forum for protecting sensitive information when appropriate."

2008-2009

DR. KATHLEEN KIERNAN served as the second Chair of the InfraGard National Members Alliance (INMA) Board of Directors from July 2008 to October 2012.

Dr. Kiernan was the founder and CEO of Kiernan Group Holdings, Inc. and a 29 year veteran of Federal Law Enforcement. She had previously served as the Assistant Director for the Office of Strategic Intelli

gence and Information for the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) where she was responsible for the design and implementation of an intelligence-led organizational strategy to mine and disseminate data related to explosives, firearms and illegal tobacco diversion, the traditional and non-traditional tools of terrorism.

Dr. Kiernan completed her Doctorate in Education at Northern Illinois University and her Master of Science in Strategic Intelligence at the Joint Military Intelligence College in Washington, D.C. She also holds a Master of Arts in International Transactions from George Mason University Homeland Security Policy Institute and a faculty member at The Johns Hopkins University and the Naval Postgraduate School Center for Homeland Defense and Security.

Under Chairwoman Kiernan, Ron Dick served one year as INMA President.

RONALD L. DICK served as President of INMA from 2008 to 2009. He retired from the FBI after serving twenty-five years in law enforcement. Ron served as a Senior Executive as Director of the National Infrastructure Protection Center (NIPC) and Deputy Assistant Director (DAD) of the Counterterrorism (CT) and Cyber Crimes Division (CCD). As Director of the NIPC, he was responsible for the coordination of the detection, assessment, warning, response and investigation of all cyber and physical threats to the critical infrastructures of the United States. As the Deputy Assistant Director for CT & CCD, he developed and executed the FBI's domestic and international infrastructure protection efforts and responded to criminal, terrorist and nation-sponsored cyber threats against the United States Government and private industry.

Mr. Dick has a Bachelor of Science Degree in accounting from New Mexico State University.

Dr. Kiernan listed major accomplishments under her leadership as follows:

1. Bridging the public-private divide to identify and share best practices in an emergent threat environment.
2. Introducing and facilitating cross-sector coordination
3. Sponsoring "Thought Leadership Forums" at the National Press Club that hosted talks by key leaders including the Cyber Czar; General Shields (JIEDDO), FEMA Director Craig Fugate; USCG Commandant Thad Allan and Congressional Representatives Silvestre Reyes and Michael Rogers.
4. Providing an opportunity for continued public service to our country.
5. Championing the recruitment of younger members at university level.
6. Recruiting top flight national board members.
7. Supporting the expansion of multi-regional partnerships in Arizona and California; and
8. Forging a strong relationship with the Orange County Choppers (OCC) partnership with the FBI and Hudson Valley Chapter of InfraGard, helping organize a major fundraising effort through the sale of a specially made motorcycle to raise awareness and support the Newburgh youth avoid gangs and reduce the violent crime that is synonymous with the gang culture. There are approximately one million gang members belonging to more than 20,000 gangs in the U.S. Newburgh led the state in violent crimes per capita. This was a unique initiative to reach out to the youth and help provide them with opportunities to steer

their future in the right direction. Dr. Kiernan said projects like this reinforce our private sector partnerships with the public and educate our youth that early bad decisions can impact future opportunities to change the world.

INMA signed MOU with IT ISAC (Information Technology Sector Information Sharing and Analysis

Ms. Dyann Bradbury

2009-2010

DYANN R. BRADBURY served as INMA President from 2009 to 2012. She previously served as INMA Executive Vice President for Regional Affairs in 2007 and as an INMA Director in 2008. She was a Past President and Vice President of the InfraGard Nebraska Members Alliance and served in other assignments for both INMA and Nebraska.

Ms. Bradbury is a Senior Director of Corporate Compliance for Digital River. In this role, responsibilities include Import and Export compliance, PCI-DSS and PA-DSS compliance, SSAE16 and SO2 audits, review of global data privacy, data protection and data breach law.

Doug Callen served as Advisory Board Chair during Don Gilbert's medical leave.

In a December 1, 2009, FBI press release issued at an InfraGard Hudson Valley Members Alliance meeting, the Bureau demonstrated its continuing enthusiasm for the program and gratitude to all members of the Hudson Valley team. Joseph Demarest, the Assistant Director in Charge of the FBI New York

Division at that time, stated:

> "In the one year since the Hudson Valley Chapter was established, we have had multiple success stories. One accomplishment is the identification of key individuals who are currently providing information on criminal and terrorism threats inside and outside the region. As always, communication from our members remains a vital resource for the FBI. We'd thank our InfraGard partners for their continued commitment and dedication to our community and our country."
>
> *https://www.fbi.gov/newyork/press-releases/2009/infraGard-hudson-valley-members-alliance-meeting*.

Ms. Sheri Donahue

2011-2012

September 20, 2011 – INMA announced the launch of a nationwide special interest group (SIG) that will focus on threats that could cause nationwide long-term critical infrastructure collapse. Named the EMP SIG, after electromagnetic pulse, the SIG will cover all similarly dangerous hazards such as extreme space weather, coordinated physical attack, cyber-attack or pandemics. Charles Manto served as Chair.

2013-2014

DAVID PEKOSKE served as the INMA Board Chair from 2013 to 2015. He was a Vice Admiral and assumed the duties as Vice Commandant of the United States Coast Guard on August 7, 2009. As second in command and Chief Operating Officer, Vice Admiral Pekoske executed the Commandant's strategic intent, managed internal organizational governance and served as the Component Acquisition Executive. His thirty-two plus year career has included a variety of operational and staff assignments and command of six Coast Guard operational units. He served on the west, gulf and east coasts of the United States and on the Great Lakes. Vice Admiral Pekoske's operational expertise is in the operations ashore community.

Commissioned in 1977, Vice Admiral Pekoske has a Bachelor of Science Degree in Ocean Engineering from the United States Coast Guard Academy. He was a 1989 graduate of the School of International and Public Affairs at Columbia University with a Master's Degree in Public Administration, and graduated

from the Sloan School of Management at the Massachusetts Institute of Technology with an MBA in 1997.

SHERI DONAHUE served as President during Pekoske's term as Chairman.

Sheri Donahue had been an active member of InfraGard since 2003. She was part of the National Board

of Directors since 2004 in various roles: as a member of the Board, as the first Managing Director, and as an officer of the corporation - Secretary (2004-2010) and President (2013-2015). Sheri received her Bachelor's Degree in Industrial Engineering from Purdue University in 1990. She served as an engineer and special programs manager for the Department of the Navy for sixteen years coordinating program protection efforts for several Navy projects, working closely with the intelligence community in the protection of Navy and DOD technologies as well as homeland security efforts.

The teamwork of Pekoske and Donahue during their tenure led to a number of accomplishments, including:

- Developing and publishing a comprehensive strategy for INMA. This strategy established a solid foundation for the smooth functioning of the INMA, recognized our unique reach across all critical infrastructure sectors and took a "national asset" approach to bringing the InfraGard public/private sector partnership across the interagency to designated Sector Specific Agencies.
- Improving communications throughout the organization through a revitalized regional representative network, quarterly newsletters and record participation levels by IMAs at Congress. Coordinated with the NIPU to ensure the annual FBI InfraGard Coordinators conference was held coincident with the Congress to enhance FBI/INMA/IMA coordination. Congress was lengthened from one to three days to take full advantage of the opportunity to meet face-to-face and work to build the FBI/INMA/IMA partnership.
- Establishing a Sector Chief program at every IMA to better organize our volunteer effort across all critical infrastructure sectors and provide ready access to our subject matter experts for field office SACs.
- Weathering the impacts of sequestration on our appropriated funding support. Aligned the INMA FY to the Government FY. Negotiated renewals of the cooperative agreement with the FBI that preserved needed flexibility for the INMA to operate while providing effective oversight and control for the Bureau

.

- Initiating the discussion with the new FBI Director and Deputy regarding the organizational placement of the InfraGard program within the office of the Director.
- Implementing an IMA certification program to ensure all IMAs met minimum requirements for operation. This ensured financial integrity, legal compliance for incorporation at the state level, director and officer insurance and

Mr. Gary Gardner

compliance with our licensing agreement with the FBI for use of the InfraGard logo and name.

- Completing a comprehensive review of the INMA By-Laws and identified areas where additional policy guidance from the INMA was warranted.
- Establishing minimum requirements for member participation and refreshed the membership rolls of the INMA so that only active members were included.
- Improving the annual awards program to provide more visibility and participation in the nomination and selection process. Funded the participation of all award winners to be present at the awards ceremony at Congress and obtained the Director's participation in this important event.
- Reorienting of the advisory council so that its membership would include thought leaders from the public and private sector to advise the INMA and FBI as well as enhance the brand of InfraGard in the critical infrastructure space.

IGuardian Launched.

In an effort to enhance the FBI's ability to mitigate and prevent serious cyber threats, the FBI launched a new, secure portal to allow industry partners to quickly and safely report actual and attempted cyber intrusion incidents. Called iGuardian, the information portal was similar to eGuardian, a sensitive but unclassified platform for law enforcement partners to provide potential terrorism-related threats and suspicious terrorism-related activity reports. iGuardian greatly sped up the process of submitting intrusion information to the FBI. Within minutes of submitting the form electronically, agents and analysts quickly triage the submissions, notify previously unknown intrusion victims, and assign leads as appropriate to Field Offices for further investigation. The information in iGuardian also provided a big picture look at the threat from terrorists, nation states, and criminal groups conducting complex cyber network operations against the United States.

2015-2016

GARY GARDNER became INMA Chair in September 2015. He has been President of TotaleAccess, a security and investigations firm in Charlotte, North Carolina since 2005 and served as Director of Security for NASCAR from 2005 to 2008. Gary has volunteered as a member of the InfraGard Charlotte Members Alliance since 2001 including serving as President. He owns and operates a cybersecurity consulting company.

DR. EARL J. MOTZER became INMA Vice Chairman in October 2015. He previously served as Vice President and Healthcare and Public Health Sector Chief for the InfraGard Kentucky Members Alliance and previously served as the National President of the FBI National Citizens Academy Alumni Association. Motzer retired after leading hospitals and nursing homes for 50 years and serving as an adjunct graduate school faculty member for 41 years.

JERRY L. BOWMAN became President and CEO of INMA in September 2015. He has been Chief Business Development Officer at Innovative Management and Technology Approaches, Inc. In Washington,

D.C. since September 2015. Prior to that he was Executive Vice President at ICS Nett, Inc. from February 2012 to September 2015 and in various management positions with BICSI from 2006, including President from February 2012 to February 2014.

- CHAPTER NINE -

INFRAGARD TODAY

"The way a team plays as a whole determines it success. You may have the greatest bunch of individual stars in the world, but if they don't play together, the club won't be worth a dime."

Baseball great Babe Ruth

PARTNERSHIPS

In the interest of strengthening and broadening private-sector/government cooperation in critical infrastructure protection, InfraGard National Members Alliance (INMA) forms and maintains partnerships and close working relationships. Some of INMA most important ones include:

Stop-Think-Connect Campaigns:

InfraGard is a member of the Department of Homeland Security's Stop, Think, Connect campaign, a national public awareness campaign aimed at helping to promote cyber safety in communities across the country.

National Center for Missing & Exploited Children (NCMEC):

Established in 1984, the National Center for Missing & Exploited Children is the leading nonprofit organization in the I.S. working with law enforcement, families and the professionals who serve them on issues related to missing and sexually exploited children. As part of its Congressional authorization, NCMEC has created a unique public and private partnership to build a coordinated, national response to the problem of missing and sexually exploited children, establishing a missing children hotline and serve as the national clearinghouse for information related to these issues.

EDUCATION PARTNERS

American Military University (AMU):

From natural disasters to the threat of national and international terrorism, those who protect the public must be prepared for a variety of challenges. American Military University is a leading provider of affordable, quality online education to public safety professionals looking to take the next step in their careers. Its programs will help prepare students for these demanding roles.

Excelsior College, home to the National Cyber Institute:

The Institute offers an array of cyber related programs, including a Bachelor of Science (BS) in Cyber Operations, BS in Information Technology (Cybersecuri-

ty)

and Master of Science in Cybersecurity, as well as certificate programs at the undergraduate and graduate level. Five of the college's programs have been certified to meet the National Security Agency's Committee on National Security Systems (CNSS) Training Standards, making Excelsior part of an elite group

of academic institutions.

SANS Institute:

SANS provides intensive, immersion training designed to help you and your staff master the practical steps necessary for defending systems and networks against the most dangerous threats – the ones being actively exploited.

The University of Maryland University College

University of Maryland University College (UMUC) offers undergraduate and graduate study programs to InfraGard members worldwide. UMUC is a regionally accredited globally focused university educating 92,000 students. Through the INMA-UMUC education alliance, students can pursue studies through evening and weekend classroom formats, entirely online or through a combination of both.

INFRAGARD MEMBERSHIP

In the twenty years that InfraGard has evolved, it has developed a vetted membership consisting of thousands of subject matter experts across all sixteen critical infrastructure sectors. These members include business professionals, academia, government, state, local, and tribal government, law enforcement and military dedicated to support the mission and protection of our critical infrastructure.
Each member of the 80+ local InfraGard Member Alliances (IMAs) gains an understanding of the threats posed by criminals and foreign adversaries. They have access to information and tools that will equip them with the most current best practices.

Additional member benefits include:

1. Collaboration across InfraGard membership
2. Information sharing with FBI and Law Enforcement
3. Timely intelligence briefings
4. Identification, prioritization and mitigation of vulnerabilities
5. Development of incident response plans
6. Special Interest Groups (SIGs)
7. Access to iGuardian
8. Training and education programs
9. Discounts to local seminars and conferences
10. Access to Malware Investigator

Putting together these expert members, valuable benefits, and wide-ranging partnerships has enabled InfraGard to grow from the small pilot program that started in Cleveland twenty years ago into the important role the organization plays today in working with the FBI and other federal agencies to protect America's critical national infrastructure. The next twenty years promises more of the same.

- CHAPTER TEN -

INMA TOMORROW

> "Coming together is a beginning; Keeping together is progress; Working together is success"
>
> Henry Ford

Although the future is unknowable, the InfraGard National Members Alliance (INMA) has charted its course for the future in the The INMA Strategic Plan, 2015-2020. Building upon its previous work, the Plan declares that "the InfraGard Mission is to provide a trusted exchange of information related to the protection of our nation's critical infrastructure."

Given this, the INMA Mission Statement was restated as follows:

> The INMA is to execute the InfraGard Mission through supporting partnerships and opportunities with private sector and all government agencies directly and through local InfraGard Member Alliances (IMA).

The Plan suggested the following Mission Statement for IMAs:

> The InfraGard Members Alliances (IMA) Mission is to support the InfraGard Mission by providing a local trusted exchange of information related to the protection of our nation's critical infrastructure in response to local threats.

And so follows the INMA Vision Statement:

> To be the preeminent partner for all trusted information and the leading knowledge resource in the protection of our nation's critical infrastructure.

Between 2015 and 2020, the INMA has three top priorities:

1. Partnership –
    a. Support InfraGard Members Alliances (IMAs);
    b. Foster the mission of information sharing between the FBI and Private Sector; and
    c. Attract subject matter experts to InfraGard, and establish power through partnership with InfraGard stakeholders and each IMA.
2. Governance –
    a. Protect the brand and establish InfraGard as the premier Critical Infrastructure Protection Program,
    b. Review and upgrade INMA Board of Directors and IMA Chapter governance.
3. Financial Responsibility –
    a. Monetize projects through sponsorship programs,
    b. Fund the Mission through the monetization of programs and services, c. Establish conference(s).

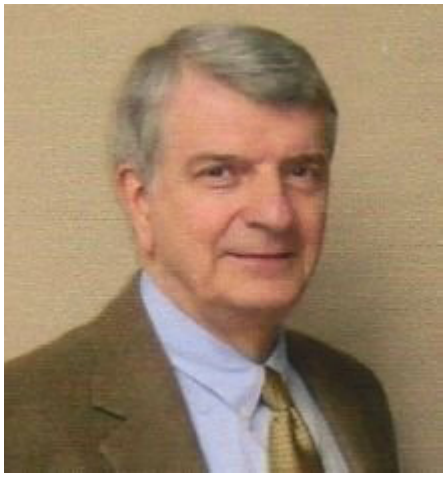
Past Chair
Phyllis Schneck

Current President
Jerry Bowman

Past Chair
Kathleen Kiernan

Past Chair
David Pekoske

KEY LEADERS



Bob Heim

Past President
Rob Schmidt

APPENDICES

A INFRAGARD MEMBERSHIP METRICS

January 6, 2001 All 56 FBI Field Offices had opened InfraGard Chapters with a total of 518 members across the nation.
May 22, 2001 Over 1200 members
July 2001 Over 1600 members
October 4, 2001 Over 2000 members
May 8, 2002 Over 4000 members
September 4, 2003 Over 8000 members
December 14, 2004 Over 14,800 members, 80+ chapters
2006 Over 16,000 members, 80+ chapters
January 2008 Over 23,000 members, 80+ chapters
March 8, 2010 Over 35,000 members, 80+ chapters
August 6, 2011 Over 40,000 members, 80+ chapters
2016 Over 48,000 members, 80+ chapters

B. INMA Leadership, 2004-2016.

2004-2005

Congress: June 28-29 at the Renaissance Hotel, Washington, DC
Conference: June 30 – July 1 at the Renaissance Hotel, Washington, DC
FBI Unit Chief: SSA Brett Hovington

INMA Board/Officers 2004-2005
Board: Dr. Phyllis Schneck, Chair
Ms. Sheri Donahue (elected)
Mr. Freeman Mendell (elected)
Mr. Keith Morales (elected)
Mr. Jeff Schmidt
Mr. Robert Schmidt
Mr. Gary Warner
Officers:
President Dr. Phyllis Schneck
Vice President Mr. Keith Morales
Secretary Ms. Sheri Donahue
Treasurer Mr. Jeff Schmidt
Committees:
Audit: Freeman Mendell, Chair; Keith Morales
Budget: Rob Schmidt, Chair; Sheri Donahue; Jeff Schmidt

Ethics: Bill Cook, Chair, (Chicago IMA President)

2005-2006

Congress: August 08 at the J.W. Marriott Hotel, Washington, DC
FBI Unit Chief: SSA Don Good

INMA Board/Officers 2005-2006
Board: Dr. Phyllis Schneck (re-elected to 3 year term), Chair
Mr. Mike Dahn (elected to 2 year term)
Ms. Sheri Donahue
Dr. Bill Flynt LTC (Ret.) (elected to 2 year term)
Mr. Richard Garcia (appointed to 3 year term)
Dr. Kathleen Kiernan (appointed to 3 year term)
Mr. Freeman Mendell
Mr. Keith Morales
Mr. Bryant Tow (elected to 3 year term)
Officers:
President: Mr. Rob Schmidt
Vice President: Mr. Keith Morales
Vice President: Mr. Bryant Tow
Secretary: Ms. Sheri Donahue
Treasurer: Mr. Jeff Schmidt
Committees:
Audit: Freeman Mendell, Chair; Keith Morales
Budget: Bryant Tow, Chair; Mike Dahn; Jeff Schmidt
Ethics: Bill Cook (Chicago IMA President), Chair

2006-2007

Congress: August 21 at the Renaissance Hotel, Washington, DC
Linda Franklin Award: Jon Miller, Long Island IMA
Conference: August 22-24 at the Renaissance Hotel, Washington, DC
FBI Unit Chief: SSA Don Good

INMA Board/Officers 2006-2007
Board: Dr. Phyllis Schneck, Chair
Mr. Mike Dahn
Dr. Bill Flynt LTC (Ret.)
Mr. Richard Garcia
Dr. Kathleen Kiernan
Mr. Paul Kurtz (appointed)
Ms. Sue Mencer (elected)
Mr. Freeman Mendell (re-elected)
Mr. Bryant Tow

Officers:

President:Mr. Rob Schmidt
Secretary:Ms. Sheri Donahue
Treasurer: Mr. Jeff Schmidt
(There was no VP this year)

Committees:
Audit: Freeman Mendell, Chair; Kathleen Kiernan
Budget: Sue Mencer, Chair; Rich Garcia, Jeff Schmidt
Ethics: Jeff Klaben (Sam Francisco IMA President), Chair
Advisory Board Chair: Michael Hershman

2007-2008

Congress:September 19 by secure video teleconference (SVTC)
Linda Franklin Award: Larry Shattuck, Michigan IMA
FBI Unit Chief: SSA Chris Dowd

INMA Board/Officers 2007-2008
Board: Dr. Phyllis Schneck, Chair
Mr. William Casey (appointed to 2 year term)
Mr. Mike Dahn (re-elected)
Mr. Ron Dick (appointed to 1 year term)
Mr. Richard Garcia
Mr. Jeff Geoffroy (appointed to 3 year term)
Dr. Kathleen Kiernan (re-appointed to 3 year term)
Mr. Paul Kurtz
Dr. Dave McIntyre (elected)
Ms. Sue Mencer
Mr. Freeman Mendell
Mr. Bryant Tow

Officers:
President:Mr. Rob Schmidt
Executive Vice President, Regional Affairs: Ms. Dyann Bradbury
Vice President Government Relations: Mr. Jerry Dixon
Vice President Corporate Communications: Mr. Alan Young
Vice President Special Events: Mr. Rob Pate
Secretary:Ms. Sheri Donahue
Treasurer: Mr. Jeff Schmidt
Managing Director – Ms. Sheri Donahue

Committees:
Audit: Freeman Mendell, Chair; Kathleen Kiernan
Budget: Rich Garcia, Chair; Sue Mencer

Ethics: Bill Cook (Chicago IMA President), Chair

2008-2009

Congress: June 02 at the Caribe Royale Conference Center, Orlando, FL
Linda Franklin Award: Ray Ivey, Charlotte IMA (posthumously)
GFIRST Conference: June 03-06 at the Caribe Royale Conference Center, Orlando, FL
FBI Unit Chief; SSA Chris Dowd

INMA Board/Officers 2008-2009
Board: Dr. Kathleen Kiernan, Chair
Mr. Zal Azmi (appointed to complete Jeff Geoffroy's 3 year term)
Ms. Dyann Bradbury (elected)
Mr. William Casey
Mr. Mike Dahn
Mr. Michael Hershman (appointed to 2 year term)
Dr. Dave McIntyre
Ms. Sue Mencer
Mr. Freeman Mendell
Mr. Mike Rolince (appointed to 3 year term)
Mr. Bryant Tow (re-elected)

Officers:
President: Mr. Ron Dick
Vice President Fundraising: Mr. Joe Calvanico
Vice President Government Relations: Mr. Jerry Dixon
Vice President Corporate Communications: Mr. Paul Page
Vice President Special Projects: Mr. Rob Pate
Vice President Regional Communications: Ms. Laurie Venditti
Secretary: Ms. Sheri Donahue
Treasurer: Mr. Freeman Mendell
Parliamentarian: Mr. Bill Casey
Managing Director: Ms. Sheri Donahue

Committees:
Audit: Freeman Mendell, Chair; Kathleen Kiernan
Budget: Dyann Bradbury, Chair; Freeman Mendell, Bryant Tow
Ethics: John Jackson (Chicago IMA President), Chair

Advisory Board Chair: Don Gilberg
Strategic Planning Committee: Bryant Tow, Chair

2009-2010

FBI Unit Chief: SSA John Ohashi

INMA Board/Officers 2009-2010
Board: Dr. Kathleen Kiernan, Chair
Mr. Zal Azmi
Ms. Donna Bucella
Mr. William Casey
Mr. Mike Dahn
Mr. Michael Hershman
Mr. Paul Joyal (elected)
Mr. Bradley Lide (elected)
Dr. Dave McIntyre
Mr. Mike Rolince
Col (Ret.) Bob Stephan
Mr. Bryant Tow

Officers:
President:Ms. Dyann Bradbury
Vice President: Mr. Rob Schmidt
Secretary:Ms. Sheri Donahue
Treasurer: Mr. Joe Calvanico
Parliamentarian: Mr. Bill Casey
Managing Director: Ms. Sheri Donahue (volunteer)

Committees:
Audit: Michael Hershman, Chair
Budget: Mike Rolince, Chair

Advisory Board Chair: Don Gilberg

2010-2011

Congress: August 15-17, San Antonio, TX
FBI Unit Chief: SSA Bob Nickel

INMA Board/Officers 2010-2011
Board: Dr. Kathleen Kiernan, Chair (re-appointed)
Mr. Zal Azmi
Mr. Alan Berg (elected)
Mr. Bill Casey
Ms. Sheri Donahue (elected)
Mr. Rich Garcia (appointed to complete Dyann Bradbury's 3 year term)
Mr. Michael Hershman (re-appointed)
Mr. Paul Joyal
Mr. Bradley Lide
Mr. Mike Rolince
Col. (Ret) Bob Stephan

Mr. Bryant Tow

Officers:

President:Ms. Dyann Bradbury
Vice President: Mr. Rob Schmidt
Secretary:Ms. Karla Hammer
Treasurer: Mr. Joe Calvanico
Managing Director: Mr. Steve Ewell

Committees:
Audit: Michael Hershman, Chair
Budget: Mike Rolince, Chair
Ethics: Dennis Kelly (South East Louisiana IMA President), Chair
Advisory Board Chair: Don Gilberg
Access Control and Exercise Committee: Rich Garcia, Chair
Certification and Accreditation Committee: Bryant Tow, Chair
Collaboration Committee: Suzanne Novak, Chair
CATE (Coordination, Awareness, Training and Education): Rob Pate, Chair
Community Outreach Committee: Laurie Venditti, Chair
Fusion Centers Committee: Paul Joyal, Chair
Nomination Committee: John Jackson, Chair
Sector Chief Committee: Sheri Donahue, Chair
Sponsorship and Funding Committee: Bradley Lide, Chair
Strategic Planning Committee: Ron Dick, Chair

2011-2012

Congress: August 8 at the Gaylord Opryland Hotel, Nashville, TN
Linda Franklin Award: Paul Joyal, Maryland IMA
Conference: August 7 at the Gaylord Opryland Hotel, Nashville, TN
FBI Unit Chief: SSA Bob Nickel

INMA Board/Officers 2011-2012
Board: Dr. Kathleen Kiernan, Chair
Mr. Zal Azmi (re-appointed)
Mr. Alan Berg
Ms. Sheri Donahue
Mr. Rich Garcia (re-elected)
Mr. Michael Hershman
Mr. Paul Joyal
Mr. Bradley Lide
Dr. Earl Motzer (elected)
Mr. Dave Pekoske (appointed to complete Bill Casey's 3 year term)
Mr. Clayton Scott (appointed)
LTC (Ret) Bob Stephan

Officers:

President:Ms. Dyann Bradbury
Vice President Fundraising: Mr. Bryant Tow

Secretary:Ms. Suzanne Hart

Treasurer: Mr. Joe Calvanico

Managing Director – Mr. Steve Ewell

Committees:
Audit: Michael Hershman, Chair
Budget: Zal Azmi, Chair; Paul Joyal; Bradley Lide
Ethics: Dennis Kelly (South East Louisiana IMA President), Chair
Advisory Board Chair: James Norton
Collaboration Committee: Suzanne Novak, Chair
Community Outreach Committee: Laurie Venditti, Chair
Nomination Committee: John Jackson, Chair

2012-2013

Congress: August, Atlanta, GA
Linda Franklin Award: Joe Concannon, New York City Metro IMA
FBI Unit Chief: SSA Bob Nickel

INMA Board/Officers 2012-2013
Board: Mr. David Pekoske, Chair (re-appointed)
Mr. Zal Azmi
Mr. Allan Berg
Mr. Rich Garcia
Mr. Brendan Healy (elected)
Mr. Michael Hershman
Mr. John Jackson (appointed to complete Sheri Donahue's 3 year term)
Mr. Paul Joyal (re-elected)
Mr. Nim Kidd (appointed)
Dr. Kathleen Kiernan
Dr. Earl Motzer
Ms. Kathleen O'Toole

Officers:
President:Ms. Sheri Donahue
Vice President: Mr. Bryant Tow
Secretary:Dr. Faith Heikkila
Treasurer: Mr. Sam Khashman
Managing Director: Ms. Kelly Woods Vaughn

Committees:
Audit: Brendan Healy, Chair; Allan Berg; Kathleen O'Toole
Budget: Zal Azmi, Chair

Advisory Board Chair: James Norton
Communications and Community Engagement: Rich Garcia and Kathleen O'Toole, Co-Chairs

Nominations Committee: John Jackson, Chair

Organization and Compliance Committee: Bryant Tow and Rob Schmidt, Co-Chairs; Michael Hershman; Kathleen Kiernan

2013-2014

Congress: September 04 via SVTC from FBI HQ, Washington, DC
Linda Franklin Award: Mary Lee Kingsley, Maryland IMA
FBI Unit Chief: SSA Ken Jones

INMA Board/Officers 2013-2014
Board: Mr. Dave Pekoske, Chair
Mr. Don Anderson (elected)
Mr. Zal Azmi
Mr. Jerry Bowman (appointed)
Mr. Rich Garcia
Mr. Brendan Healy
Mr. John Jackson
Mr. Bob Janusaitis (elected)
Mr. Paul Joyal
Mr. Sandy Mangold (appointed)
Dr. Earl Motzer
Ms. Kathleen O'Toole

Officers:
President: Ms. Sheri Donahue
Vice President: Mr. Bryant Tow
Secretary: Dr. Faith Heikkila
Treasurer: Mr. Sam Khashman
Managing Director: Ms. Kelly Woods Vaughn

Committees:
Budget: Zal Azmi, Chair
Advisory Board Chair: James Norton
Access Control Committee: Rich Garcia, Chair
Fundraising Committee: Paul Joyal, Chair
Governance Committee: Bryant Tow, Chair
Nominations Committee: John Jackson, Chair

2014-2015

Congress: September 08 at the National Conference Center, Leesburg, VA

Linda Franklin Award: Bruce Churchill, San Diego IMA
Conference: September 07 at the National Conference Center, Leesburg, VA
FBI Unit Chief: SSA John Pi

INMA Board/Officers 2014-2015

Board: Mr. Dave Pekoske, Chair
Mr. Don Anderson
Mr. Zal Azmi
Mr. Jerry Bowman
Mr. Bill Davis (appointed)
Mr. Gary Gardner (appointed)
Mr. Brendan Healy
Mr. Bob Janusaitis
Mr. Paul Joyal
Mr. Sandy Mangold
Mr. Matt Miller (elected)
Dr. Earl Motzer (re-elected)

Officers:
President:Ms. Sheri Donahue
Vice President: Mr. John Jackson
Secretary:Dr. Faith Heikkila
Treasurer: Mr. Sam Khashman
Managing Director: Ms. Kelly Woods Vaughn
Committees:
Audit: Bob Janusaitis, Chair
Budget: Bill Davis, Chair
Advisory Board Chair:
Bylaws Committee: Paul Joyal, Chair
Education Committee: Gary Gardner, Chair
Sector Chief Committee: Earl Motzer, Chair

2015-2016

Conference: September 19-20 at the Westfields Marriott, Chantilly, VA
Congress:September 21 at the Westfields Marriott, Chantilly, VA
Linda Franklin Award: David Talisman, Hawaii IMA
FBI Unit Chief: SSA John Pi

INMA Board/Officers 2015-2016
Board: Mr. Gary Gardner, Chair
Dr. Earl Motzer, Vice Chairman
Mr. Don Anderson
Mr. Jerry Bowman
Mr. Bill Davis
Mr. Jeff Gaynor (appointed)
Mr. Bob Janusaitis

Mr. Sandy Mangold
Mr. Paul Michaels (elected)
Mr. Matt Miller
Mr. Michael Poynter (appointed)

Officers:
President:Mr. Jerry Bowman
Vice President: Mr. Bill Davis
Secretary:Ms. Kimberly Pratt
Treasurer: Mr. Sam Khashman

Committees:
Audit : Matt Miller, Chair
Awards : Bradley Lide, Chair
Budget : Bill Davis, Chair
Bylaws : Gary Gardner
Education : Paul Michaels
ERM : Don Anderson, Chair
Ethics : Cindy Green Ortiz, Chair
Executive : Gary Gardner, Chair
History of InfraGard : Dr. Earl J. Motzer, Chair
Marketing & Communications : Kimberly Pratt, Chair
Nominations : Matt Miller, Chair
Resource : Jerry Bowman, Chair
Sector Chief : Jeff Gaynor, Chair
Strategic Planning : Sandy Mangold, Chair
Technology : Bob Janusitis, Chair

C. InfraGard National Executive Board (INEB) October 2001, Strategic Plan

INFRAGARD STRATEGIC PLAN
October, 2001

The National InfraGard Program began as a pilot project in 1996, when the Cleveland FBI Field Office asked local computer professionals to assist the FBI in determining how to better protect critical information systems in the public and private sectors. From this new partnership, the first InfraGard Chapter was formed to address both cyber and physical threats.

The NIPC, in conjunction with representatives from the private industry, the academic community, and the public sector, further developed the "InfraGard" initiative to expand direct contacts with the private sector infrastructure owners and operators and to share information about cyber intrusions, exploited vulnerabilities, and infrastructure threats. The initiative, encouraging the exchange of information by government and private sector members, continued to expand through the formation of additional InfraGard chapters, within the jurisdiction of each FBI Field Office. As of this date, all 56 field offices of the FBI have opened an InfraGard chapter, with hundreds of company members across the nation.

THE MISSION OF INFRAGARD

The purpose and primary objective of InfraGard is to increase the security of the United States national infrastructures through ongoing exchanges of information relevant to infrastructure protection and through education, outreach, and similar efforts to increase awareness of infrastructure protection issues. InfraGard is a Partnership between Private Industry and the U.S. government (represented by the National Infrastructure Protection Center within the FBI). The InfraGard initiative was developed to encourage the exchange of information by the government and the private sector members.
Private sector members and at least one FBI field representative form local area chapters. These chapters set up their own boards to govern and share information within the membership. Each chapter is also part of an organization which is InfraGard.

The National Infrastructure Protection Center and the Federal Bureau of Investigation play the part of facilitator by:

- gathering information and distributing it to members
- educating the public and members on infrastructure protection
- disseminating information through the InfraGard network
- producing valuable analytical products on information received through the InfraGard network
- opening the doors of communication between government and private sector members.

Within this mission statement herein, we are not only concerned with Internet security but also the great-

er arena of network security as we must assist the membership and deal with the trusted insider who has access to the inner sanctum.

THE VISION OF INFRAGARD (BY 2003):

InfraGard will become a highly-regarded partnership and definitive source of information dedicated to the protection of all critical national infrastructures. Moving forward, InfraGard shall be the designated private sector group to partner with the government to focus on the following challenges that can only be met via true partnership and information sharing:

- To facilitate a common interpretation of the roles and responsibilities of the NIPC.
- To facilitate working relationships between the FBI, NIPC, and other government security entities and key personnel to enable those entities to work together to set priorities and entity oversight.
- To formally recognize the role of the NIPC within national security warning procedures.
- To work with the NIPC to set criteria to determine when an electronic attack is appropriately considered a national security event.
- To work with the NIPC on determining the appropriate role (support or lead) for the NIPC in a national security event.
- To develop a master database of attacks seen within the private sector and the NIPC.
- A Strategy to Achieve Information Sharing

Awareness and Marketing

InfraGard will focus on raising the awareness of all appropriate groups and of bringing them into the InfraGard space.

The more parties that participate within InfraGard, the greater the knowledge and information base, and thus the greater the success of the entire initiative. It is imperative that InfraGard generate awareness of information security and critical national infrastructure protection issues while always maintaining the highest integrity. The InfraGard partnership must recruit new members, yet must never be

perceived as a commercial or political marketing venue. InfraGard has designated an internal committee to address these challenges.

InfraGard will seize opportunities to generate awareness of:

- The information security threat to critical national infrastructures
- The value in public-private partnerships in trust and plan execution
- Efforts in technology and legislation
- InfraGard as the leader in trusted public-private partnership to enable critical national infrastructure protection

InfraGard will be careful to not:

- Endorse commercial products

- Be utilized as a commercial or political marketing front

Broadening InfraGard Membership

An internal committee within InfraGard has been designated to address the following challenges no later than the end of Q4 2001:

- To clarify the current membership application to reflect decisions made at the 2001 San Diego InfraGard National Conference regarding participation levels of those who sign the Secure Access Agreement (SAA) vs. those who do not
- To clarify the procedures for corporate vs. individual memberships
- To create and instantiate policies for the formal creation and NEB acknowledgement of provisional chapters
- To clarify membership requirements for academic institutions
- To recommend a method of secure communication for those entities that do choose to enter into the SAA
- To recommend policies and procedures for non-U.S.-based employees of companies that are members

Information Exchange, Distribution and Dissemination

Information sharing begins with human relationships – people talking with people whom they trust. The public-private partnership is based on trust, generated by people getting to know one another in business as well as more casual settings such as conferences. Individual InfraGard chapters host regular

meetings on their own schedules, which introduce people in a local and community "grass roots" context. This is considered intra-chapter information exchange. Within each chapter, the InfraGard coordinator will be responsible for gathering, filtering and disseminating intra-chapter information communications as well as for coordinating the information flow into and out of the NIPC for that chapter.

Geographically proximate clusters of local Chapters will be classified into "regions," generating a higher level, inter-chapter, intra-region information exchange.

The next level of information exchange will be at the national, inter-region level.

Leveraging the Trust Network

Time and accuracy are the essential ingredients in information dissemination in an information security event. InfraGard will work within its member organizations and government partners to determine the optimal methods of distributing information in the fastest and safest manner to all member organizations nationwide. InfraGard will work with the NIPC to determine processes and procedures to identify key individuals and entities to:

- Track threats 24x7
- Ensure information integrity
- Quickly identify information security events
- Direct information security events to appropriate commercial and government entities and clearinghouses

- Provide timely warnings of events
- Provide solutions to impending threats
- Distribute information in near real-time to member organizations
- Communicate in near real-time with member organizations for updates or new information

Details are currently still being worked, with a pilot information dissemination flow policy (based on one already in existence?) set for the 2002 National InfraGard Conference.

Education Strategies

1. To protect the academic infrastructure:
    - Encourage student involvement in InfraGard on a limited basis
    - Work with University network administrators to enhance security on academic networks
2. To work with Universities and information security research centers to:
    - Generate ideas exchange in new research
    - Offer a network of public and private entities to students for educational internships and future employment in information security
    - Offer a network of public and private entities to students for potential research testbeds and pilot laboratories

Sustainability Strategies

InfraGard shall use the sustainability strategies herein to ensure the ability to implement the information sharing partnership and trust network. InfraGard shall develop appropriate mechanisms to bring external input into the NEB.

THE INSTANTIATION OF A BOARD OF ADVISORS TO THE NATIONAL EXECUTIVE BOARD

The National Executive Committee (NEC) shall designate a Board of Advisors in order to gather a pool of experts to enhance critical decisions made by the NEC.

The Advisory Board to the NEC shall have the following roles and responsibilities:

- To serve as expert resources for the NEC as requested on political, technological and tactical issues that affect critical national infrastructure protection
- To facilitate inter-agency relationships for NIPC and other government offices and entities
- To serve as supporters of the NIPC and the InfraGard initiative within other governmental agencies, corporate entities, and universities

Advisory Board placements shall be made by the NEC and voted on according to the Bylaws of the NEC.

THE DEFINITION OF THE WORKING RELATIONSHIP BETWEEN INFRAGARD AND THE ISACS

InfraGard represents the grass roots membership in information sharing. We shall work in parallel and constant communication with the IT-ISAC, and eventually the other ISACs, as defined by a procedure to be developed within the coming year.

THE INTERNATIONAL EXPANSION OF INFRAGARD: GLOBAL INFORMATION EXCHANGE

Information security and critical infrastructure protection is a global challenge, and is not limited by American borders. As the InfraGard partnership evolves into an authoritative and active partnership for trusted information sharing,

To address the following challenges in information sharing and communication with:

- Entities incorporated in the United States with office abroad
- Entities incorporated abroad with offices in the United States
- Information sharing across National borders, starting with friendly nations, to protect National as well as foreign infrastructures

Moving forward, InfraGard must eventually work with international law enforcement and legislative bodies to enable international communication into the information exchange and distribution policies.

The Strategic Role in the Community for InfraGard:

- To generate awareness of information security and the threats to our critical national infrastructures
- To facilitate partnership between law enforcement, government, industry and academia whenever and wherever possible
- To support efforts in education, teaching students to be responsible about cyber activities and networking from K-12 and higher
- To support research in information security and to help utilize that work wherever possible.

The InfraGard National Executive Board would like to thank Dr. Peter Freeman, member of the InfraGard Atlanta Board of Directors and John P. Imlay, Jr. Dean of Computing at Georgia Tech, for their assistance and direction in strategic planning.

D. First Memorandum between FBI and InfraGard National Members Alliance (INMA) 2004

MEMORANDUM OF UNDERSTANDING
Between
The Federal Bureau of Investigation
and
The InfraGard National Members Alliance

I. BACKGROUND AND PURPOSE

THIS MEMORANDUM OF UNDERSTANDING (MOU) OUTLINES AREAS IN WHICH THE FEDERAL BUREAU OF INVESTIGATION (FBI) AND THE INFRAGARD NATIONAL MEMBERS ALLIANCE (INMA) ARE COOPERATING, AND PLAN TO COOPERATE, TO INCREASE THE SECURITY OF THE UNITED STATES NATIONAL INFRASTRUCTURE THROUGH ONGOING EXCHANGES OF INFORMATION RELEVANT TO CRITICAL INFRASTRUCTURE PROTECTION AND THROUGH EDUCATION, OUTREACH, AND SIMILAR EFFORTS TO INCREASE AWARENESS OF INFRASTRUCTURE PROTECTION ISSUES. THIS MOU ALSO DEFINES AND CLARIFIES CERTAIN RIGHTS AND RESPONSIBILITIES THAT EXIST BETWEEN THE INMA, ITS MEMBERS (THE INFRAGARD MEMBERS ALLIANCES), AND THE FBI.

A. NATURE OF INFRAGARD: INFRAGARD IS AN FBI PROGRAM DEDICATED TO PROMOTING ONGOING DIALOGUE AND TIMELY COMMUNICATION BETWEEN THE PRIVATE SECTOR AND THE FBI CONCERNING CRITICAL INFRASTRUCTURE PROTECTION ISSUES. THE FBI AND INFRAGARD MEMBERS ARE ENGAGED IN THIS COOPERATIVE UNDERTAKING IN RECOGNITION THAT A PUBLIC/PRIVATE STRATEGIC PARTNERSHIP IS OF VITAL IMPORTANCE TO OUR NATION'S SECURITY.

B. ROLES OF THE FBI AND THE INMA IN INFRASTRUCTURE PROTECTION: THE PARTIES UNDERSTAND THAT CRITICAL INFRASTRUCTURE PROTECTION IS ACHIEVED BY ELIMINATING OR REDUCING THREATS, ELIMINATING OR REDUCING VULNERABILITIES, AND ELIMINATING, REDUCING, OR MANAGING THE NEGATIVE CONSEQUENCES OF A SUCCESSFUL ATTACK AGAINST THE UNITED STATES.

THE FBI'S CRITICAL INFRASTRUCTURE ROLE IS FOCUSED PRIMARILY ON THREAT REDUCTION, BY PRE

VENTING ATTACKS WHENEVER POSSIBLE AND BY DETERMINING ATTRIBUTION WHEN ACTUAL OR ATTEMPTED ATTACKS OCCUR. FBI INVESTIGATIONS ALSO MAY REVEAL INFORMATION PERTINENT TO VULNERABILITY MITIGATION EITHER BY DISCOVERING VULNERABILITIES THAT ARE FIRST REVEALED DURING AN INVESTIGATION, OR BY ASSISTING IN PRIORITIZATION EFFORTS BY DETERMINING WHICH VULNERABILITIES ARE BEING TARGETED BY THREAT ACTORS.

THE INMA, NATIONALLY AND THROUGH ITS LOCAL INFRAGARD MEMBERS ALLIANCES,

REPRESENTS THE PROGRAM INTERESTS OF THE THOUSANDS OF PRIVATE SECTOR INFRAGARD MEMBERS LOCATED THROUGHOUT THE UNITED STATES. THE ROLE OF THE PRIVATE SECTOR IN CRITICAL INFRASTRUCTURE PROTECTION IS AS BROAD AS IT IS SIGNIFICANT. AS STATED IN THE JULY 2002 NATIONAL STRATEGY FOR HOMELAND SECURITY, THE PRIVATE SECTOR IS A "KEY HOMELAND SECURITY PARTNER," BEING "THE NATION'S PRINCIPAL PROVIDER OF GOODS AND SERVICES AND OWNER OF 85 PERCENT OF OUR INFRASTRUCTURE." THE NATIONAL STRATEGY CONTINUES, "AN INFORMED AND PROACTIVE CITIZENRY IS AN INVALUABLE ASSET FOR OUR COUNTRY IN TIMES OF WAR AND PEACE. VOLUNTEERS ENHANCE COMMUNITY COORDINATION AND ACTION, WHETHER AT THE NATIONAL OR LOCAL LEVEL. THIS COORDINATION WILL PROVE CRITICAL AS WE WORK TO BUILD THE COMMUNICATION AND DELIVERY SYSTEMS INDISPENSABLE TO OUR NATIONAL EFFORT TO DETECT, PREVENT, AND, IF NEED BE, RESPOND TO TERRORIST ATTACK." INDIVIDUALLY AND COLLECTIVELY, INFRAGARD MEMBERS HAVE VOLUNTEERED TO WORK WITH THE FBI TO PROTECT OUR NATION'S CRITICAL INFRASTRUCTURE IN ORDER TO DETECT, PREVENT, AND, IF NEED BE, RESPOND TO TERRORIST ATTACK.

II. UNDERSTANDING OF THE PARTIES

A. ORGANIZATION OF THE INMA. THE PARTIES ACKNOWLEDGE THAT THE INMA WILL BE ORGANIZED AND SHALL OPERATE EXCLUSIVELY WITHIN THE MEANING OF SECTION 501(C)(3) OF THE INTERNAL REVENUE CODE. THE PARTIES ALSO ACKNOWLEDGE THAT THE INMA WILL BE ORGANIZED INTO INDIVIDUALLY INCORPORATED INFRAGARD MEMBERS ALLIANCES (IMAS) ALSO OPERATING EXCLUSIVELY WITHIN THE MEANING OF SECTION 501(C)(3). IN THIS REGARD, THE INMA AND ITS MEMBER IMAS WILL BE STRICTLY PROHIBITED FROM ENGAGING IN POLITICAL ACTIVITIES.

B. INFRAGARD IS AN FBI REGISTERED SERVICE MARK. THE PARTIES ACKNOWLEDGE THAT INFRAGARD IS A REGISTERED SERVICE MARK OF THE FBI WHICH IS AND SHOULD BE CLOSELY REGULATED AND USED ONLY BY WRITTEN AGREEMENT AND IN STRICT ACCORDANCE WITH WRITTEN FBI GUIDANCE. TO ADVANCE THE INFRAGARD PROGRAM, THE FBI INTENDS, THROUGH A SEPARATE WRITTEN AGREEMENT, TO LICENSE TO THE INMA A ROYALTY-FREE, PERPETUAL, NON ASSIGNABLE, NON-TRANSFERABLE, NON-EXCLUSIVE, LICENSE TO USE THE "INFRAGARD" SERVICE MARK WITHIN THE CORPORATION'S OFFICIAL NAME, "INFRAGARD NATIONAL MEMBERS ALLIANCE," SUBJECT TO THE INMA'S ADOPTION AND ADHERENCE TO BY-LAWS THAT CONTINUE TO MEET WITH THE APPROVAL OF THE FBI. THE FBI ALSO INTENDS TO AUTHORIZE THE INMA TO SUB-LICENSE TO ITS MEMBERS THE RIGHT TO USE THE "INFRAGARD" SERVICE MARK WITHIN AN FBI-APPROVED STANDARD CORPORATE NAMING CONVENTION.

C. FBI SUPPORT OF THE INFRAGARD PROGRAM. THE FBI INTENDS TO MAINTAIN A DESIGNATED PROGRAM MANAGER AT FBI HEADQUARTERS IN WASHINGTON, DC WHO WILL COORDINATE WITH THE INMA REGARDING NATIONAL LEVEL DECISIONS CONCERNING THE INFRAGARD PROGRAM. THE FBI ALSO INTENDS THAT EACH OF ITS FIELD OFFICES THROUGHOUT THE UNITED STATES WILL HAVE AT LEAST ONE DESIGNATED SPECIAL AGENT INFRAGARD COORDINATOR, WHO WILL COORDINATE WITH LOCAL INFRAGARD MEMBERS ALLIANCES AND LOCAL INFRAGARD MEMBERS WHEN MAKING DECI

SIONS AT THE LOCAL INFRAGARD CHAPTER LEVEL.

D. INFRAGARD MEMBERSHIP. THE PARTIES ACKNOWLEDGE THAT INFRAGARD MEMBERSHIP WILL BE DETERMINED AND CONTROLLED BY THE FBI, AND THAT THE FBI INTENDS TO COORDINATE WITH THE INMA SHOULD IT DEVELOP OR REVISE STANDARDS FOR MEMBERSHIP QUALIFICATION OR DISQUALIFICATION. THE PARTIES ACKNOWLEDGE THAT, CONSISTENT WITH INMA BY-LAWS AND POLICY, QUALIFICATION FOR INFRAGARD MEMBERSHIP SHALL INCLUDE AFFILIATION WITH AN IMA. THE PARTIES FURTHER ACKNOWLEDGE THAT INFRAGARD MEMBERS GENERALLY SHALL HAVE THE RIGHT TO VOTE DIRECTLY AS TO LOCAL IMA MATTERS, AND TO VOTE INDIRECTLY THROUGH THEIR IMA REPRESENTATIVES AS TO NATIONAL INMA MATTERS.

E. INMA OVERSIGHT OF IMAS. THE PARTIES INTEND THAT THE INMA, THROUGH ITS BOARD OF DIRECTORS, WILL EXERCISE OVERSIGHT RESPONSIBILITY OF THE IMAS IN ORDER TO ENSURE THAT THE PRIVATE SECTOR'S PARTICIPATION IN THE INFRAGARD PROGRAM IS CONSISTENT WITH FBI AND INMA NATIONAL POLICY, GUIDELINES, AND LAW.

F. INMA AND IMA STRATEGIC PARTNERSHIPS. THE PARTIES ANTICIPATE THAT THE INMA AND THE IMAS, ACTING FOR PURPOSES RELATING TO U.S. CRITICAL INFRASTRUCTURE PROTECTION, WILL ENTER INTO STRATEGIC PARTNERSHIPS ON THEIR OWN BEHALF WITH ENTITIES OTHER THAN THE FBI. THE PARTIES INTEND THAT ONLY THE INMA BOARD OF DIRECTORS WILL BE AUTHORIZED TO ESTABLISH AGREEMENTS ON BEHALF OF THE INMA OR ANY IMA WITH INFRAGARD STRATEGIC PARTNERS AT THE NATIONAL LEVEL.

G. COSTS AND FINANCIAL OBLIGATIONS. THE PARTIES ACKNOWLEDGE AND AGREE THAT THIS MOU IS NOT AN OBLIGATION OR COMMITMENT OF PERSONNEL OR FUNDS, NOR A BASIS FOR A TRANSFER OF FUNDS, BUT RATHER IS A STATEMENT OF THE UNDERSTANDINGS AMONG THE PARTIES. UNLESS OTHERWISE AGREED IN WRITING, EACH PARTY IS TO BEAR ITS OWN COSTS IN RELATION TO THIS MOU. EXPENDITURES BY EACH PARTY ARE SUBJECT TO ITS BUDGETARY PROCESSES AND TO THE AVAILABILITY OF FUNDS AND RESOURCES PURSUANT TO APPLICABLE LAWS, REGULATIONS, AND POLICIES.

H. UNDERSTANDING OF THE PARTIES/NO THIRD PARTY RIGHTS. ALTHOUGH THE PARTIES ACKNOWLEDGE THAT THIS MOU IS NOT ENTERED INTO AS A LEGALLY BINDING AGREEMENT, NOR AS A FORMAL EXPRESSION OF A LEGALLY BINDING AGREEMENT, IT IS AN EXPRESSION OF THE PURPOSE AND INTENT OF THE PARTIES CONCERNED. SIMILARLY, THIS MOU DOES NOT CONFER, GRANT, OR AUTHORIZE ANY RIGHTS, PRIVILEGES, OR OBLIGATIONS AS TO ANY THIRD PARTIES OTHER THAN AS IT MAY DESCRIBE THE UNDERSTANDING OF THE PARTIES ABOUT THE RELATIONSHIP OF THE FBI, THE INMA, THE IMAS, AND INFRAGARD MEMBERS.

I. AMENDMENT AND TERMINATION. THIS MOU MAY BE AMENDED AT ANY TIME BY MUTUAL, WRITTEN CONSENT OF THE SIGNATORY PARTIES THROUGH THEIR AUTHORIZED REPRESENTATIVES. THIS MOU BECOMES EFFECTIVE UPON THE LAST DATE OF SIGNATURE BY THE DULY AUTHORIZED REPRESENTATIVES OF THE PARTIES NOTED BELOW AND CAN BE TERMINATED BY DELIVERY OF WRITTEN NOTICE BY EITHER PARTY.

APPROVED AND DATED:

_____

_____
FEDERAL BUREAU OF INVESTIGATION
DATE
GAIL SEAVEY, SECTION CHIEF

_____
_____
FEDERAL BUREAU OF INVESTIGATION
DATE
OFFICE OF THE CHIEF CONTRACTOR OFFICER

_____
_____
INFRAGARD NATIONAL MEMBERS ALLIANCE
DATE
PHYLLIS SCHNECK, PRESIDENT

E. Chapter Histories

All IMA Presidents were invited by INMA in March 2016 to prepare one page histories of their IMAs to appear in this history text and the following six IMA Presidents chose to do so with our appreciation.

InfraGard Central Ohio Members Alliance History

IMA Name:

InfraGard Central Ohio Members Alliance (originally Central and Southern Ohio InfraGard Chapter; 48 counties)

IMA Location/City & State:

Columbus, Ohio

Month / Year IMA Established:

Ohio Supercomputer Center says it was active in the formation of the chapter and our first meeting in November, 1999. Brian Moeller says "1999". Someone told me "the year after the Cleveland pow-wow", which would have made it 1997. According to the President's National Security Telecommunications Advisory Committee's "LEGISLATIVE AND REGULATORY GROUP - Telecommunications Outage and Intrusion. Information Sharing Report" dated June, 1999 (which means it must pre-date November, 1999):

> "The National InfraGard Program began as a pilot project in summer 1996 in Cleveland, Ohio. The National InfraGard Program is currently composed of local InfraGard chapters in Cleveland and Columbus, Ohio, and Indianapolis, Indiana. (The Columbus and Indianapolis chapters are recent additions to the national program.)"
> (*https://www.dhs.gov/sites/default/files/publications/Legislative%20and%20Regulatory%20Group%20Report*_1999.pdf)

Current President:

Clifford Collins

Name of Person Providing Information:

Stephen Malott

Address:

P.O. Box 361162, Columbus, OH 43236-1162

Names of Founding Board Members/Officers:

Brian Moeller, Bill Yang, Steve Romig – maybe also Matt Curtain and Mowgli Assor

FBI Field Office:

Cincinnati

Major Accomplishments of Historical Note:

One of first chapters to embrace "all-hazards" instead of cyber-centric focus. Self-sustaining, consistent membership growth, solid foundation with no pauses in sharing information with the community. Forged positive partnerships with State and County Homeland Security offices as well as local law enforcement and other governmental agencies.

InfraGard Cincinnati Members Alliance History

IMA Name:
InfraGard Cincinnati Members Alliance
IMA Location/City & State:
Cincinnati, Ohio

Month / Year IMA Established:
Rollout November 1999; 1st Meeting December 1999 Chartered in Ohio May 2005

Current President:
Arthur Foreman

Name of Person Providing Information:
Arthur Foreman

Email Address:
cincinnati.infragard@gmail.com

Names Of Founding Board Members/Officers:
Larry Lauer, Rick Martz, Jim Downing

FBI Field Office:
Cincinnati

Founding SAC Name:
Sheri Farrar

First FBI IG Coordinator Name:
Matt Drake and Roger Wilson

Major Accomplishments of Historical Note:

- Participated in opening of Dayton FBI office
- Created Digital Forensics Working Group (Cincinnati IMA special interest group)
- Obtained $20,000 grant from Ohio Criminal Justice Services for computers and printers to support InfraGard in Cincinnati, Columbus, and Dayton
- Contributed to the I-SAFE internet safety program for parents and schools and trained InfraGard members to deliver the program.

InfraGard Louisiana Members Alliance History

IMA Name:
InfraGard Louisiana Member's Alliance (ILMA)

IMA Location/City & State:
New Orleans Louisiana

Month / Year IMA Established:
April 2005

Current President:
Lester J. Millet, III

Name of Person Providing Information:
Lester J. Millet, III

Names of Founding Board Members/Officers:
Henry Newton (President), Felix Loicano (V.P), Robert Barkerding (Treasurer& BoD), Jay Smith (Membership Coordinator & BoD), Nancy Rowland Nahan, (Secretary & BoD), & Richard Bordner (Membership Coordinator)
Others: Dennis Kelly (President), Dr. Robert Muller M.D. (BoD)

FBI Field Office:
FBI New Orleans

Founding SAC Name:
Jim Bernazzani

First FBI IG Coordinator Name:
SA Will Hatcher

Major Accomplishments of Historical Note:

- Developed the Louisiana State Police Next Generation Re-Entry Protocol, which utilizes a NIMS / ICS* compliant statewide placarding system to allow for seamless transition through multi jurisdictions. Note: Mississippi has adopted this protocol and it is one protocol recognized by Louisiana State Police www.LSP.org for Parish Wide Re-entry.
- Developed the Louisiana School Safety Initiative Multi-Hazard Toolkit that provides school jurisdictions guidance on developing a comprehensive school safety program. Currently being reviewed for use as a national model.
- Conducted the largest ever Full Scale Exercise: 2010 Gulf South Crisis Area Access Control Full Scale Exercise – April 6-7, 2010
- Hosted Two very successful FBI / WMD Conferences: June 29-July 01, 2010 & May 21-23 2012- FBI INLETS (Intel & LE Training Seminar) was modeled after these events.
- 2015 Coordinator of the Year: SA Corey Harris.
- 2014 LTC Governor's Technology Award –"Growth Organization of the Year" Lester Millet III, President, InfraGard Louisiana.

InfraGard Michigan Members Alliance History

IMA Name:
InfraGard Michigan Members Alliance, Inc.

IMA Location/City & State:
Michigan

Month / Year IMA Established:
September 2002

Current President:
Bridget Kravchenko

Name of Person Providing Information:
Dr. Faith Heikkila, Chairman of the Board

Names of Founding Board Members/Officers:

John Sheridan -- President; Larry Shattuck -- Vice President; John Montville -- Treasurer; Jay Berg – Secretary.

Regarding initial support – Chris Hogan (Daimler) was instrumental in getting us an initial grant from Daimler for approx. $8k; was a huge help in getting us started and off the ground. The firm of Clark Hill incorporated us – 7/25/02. Others also contributed significantly to keep the ball rolling (i.e., Tony Robinson kicked in $1,000 to cover some expenses). The initial legal work was done primarily by Chrysler's legal department. We also had an informal group that acted like advisors but had a different designation. Mostly made up of the original organizational group that did not serve on the first board.

Two items of note in formation of the Chapter and the initial board; it was decided for coordination of activities and to minimize expenses that Michigan operate as one chapter.

Also, during the formation of the initial board we made a decision to have only one automotive company representative on the board in an effort to be more diverse.

John Sheridan might be referred to as the Father of the Michigan Chapter as he managed the creation of the organization from the member side and coordinated with the FBI as appropriate.

FBI Field Office:
Detroit

Founding SAC Name:
John Bell – 05-22-02

First FBI IG Coordinator Name:

Richard (Rick) Smith. Richard (Rick) Rytman was also engaged early on but he came on as Coordinator a few years later). They really did a great job for us as we began the effort. Richard (Dick) Murray (Assistant US Attorney – State of MI at the time) was a strong supporter/organizer of our chapter as well.

Major Accomplishments of Historical Note:

- Due to the vast area the Michigan IMA covers, quarterly meetings are broadcast to five locations in Michigan (4 Davenport University campuses – Grand Rapids, Lansing, Livonia, and Warren, along with Northern Michigan University in Marquette) using technology to show the speakers, their presentations, board members, and others in attendance at the meeting locations– this allows members to network and attend the meetings at a location nearest them;
- Offered an impactful, annual revenue generating "securing critical infrastructures" conference – providing education through nationally recognized speakers and subject matter experts for members/non-members;
- Held a members-only annual meeting at Detroit SecureWorld Expo; Michigan IMA has established a number of Sector Chiefs (financial, food & agriculture, education, healthcare, manufacturing, transportation, and government);
- Proved willing to serve on national board positions/committees and as the Midwest regional representative for more than 10 years of service combined;
- In an effort to support and promote security awareness events/activities throughout the state, our IMA develops partnerships and collaborates with local security organizations (SecureWorld, ISACA, ISSA, HTCIA, etc.);
- Exponential growth prior to revetting and also after the 2014 revetting of members.

InfraGard New Jersey Members Alliance History

IMA Name:

New Jersey Infragard Chapter, Inc.

IMA Location/City & State:

Newark, New Jersey

Month / Year IMA Established:

1998 (we do not know the month and although there is a lot of "recalling" of 1997 events, we cannot find anything "tangible" to document that the NJ Chapter was begun in1997).

Current President:

Jody Washkewicz

Name of Person Providing Information:

The following have provided the information: Bob Almberg, Les Morton, Gideon Lenkey, Dan Tum-Suden, Donna Parsons, Cochi Ho, Barbara Farrington, and Jody Washkewicz provided some and compiled the information.

Email Address:

njinfragard2002@gmail.com

Names of Founding Board Members/Officers:

Les Morton (PSE&G) – Chair; Andy Rosenau (Princeton University) -- Vice Chair; Scott Christie (McCarter & English) – Secretary; Membership Committee Members -- Renato Delatorre

(TD Waterhouse Securities) – Chair, Gideon Lenkey – RA Security, Linda Frisch - AT&T Corporate Security, John Piper – Exxon, Daniel TumSuden – IBM.

FBI Field Office:

Newark, NJ.

Founding SAC Name:

FBI SAC William Megary

First FBI IG Coordinator Name:

Steve Foster
(Followed by James O'Neil, Barbara Farrington. Current coordinator, Ed Quinn.)

Major Accomplishments of Historical Note:

- Former IG coordinator, Jim O'Neil related this story as to why Infragard is spelled "Infragard" and not "Infraguard." The naming and spelling was written that way, as Jim told me that he told by another early FBI peer, so that a slogan could be developed. This slogan, and I am paraphrasing here, was: InfraGard, protecting the nation's infrastructure. The only thing

- missing is “U” (you).
- When president of the chapter and when ID cards were issued, former NJ IMA, President, Les Morton, was issued InfraGard membership card #1.
- 2005: The NJ Chapter received an “Exceptional Service in the Public Interest” award from then Director Robert Muller.
- 2006: The NJ Chapter received a letter from then Director Robert Muller thanking both then president Gideon Lenkey and coordinator Jim O’Neil for their work involving increase local police departments’ awareness to the vulnerabilities associated with internet connected patrol cars.
- In the inaugural year of the award, Barbara Farrington was recognized by the FBI as The Best FBI Infragard Coordinator.


ESTABLISHED 1996
INFRAGARD
A KNOWLEDGE RESOURCE IN THE PROTECTION OF OUR NATION'S CRITICAL INFRASTRUCTURE
A TRUSTED INFORMATION AND
PARTNERSHIP FOR PROTECTION
LEADING PARTNER FOR
20TH ANNIVERSARY


CHEMICAL
COMMERCIAL FACILITIES
COMMUN-ICATIONS
MANUFACT-URING
DEFENSE INDUSTRIAL
DAMS
EMERGENCY SERVICES
ENERGY
FINANCIAL
AGRI-CULTURE
GOVERNMENT FACILITIES
PUBLIC HEALTH
INFO TECH
NUC, MAT & WASTE
TRANS-PORTATION
WATER
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
2
YEARS