InfraGard: On the Front Line of Critical Infrastructure Protection

Editor-in-Chief's Interview with Maureen O'Connell, President of the InfraGard National Members Alliance

Maureen O'Connell oversees the largest partnership committed to security of the nation's 16 critical infrastructure sectors. This is achieved through the mobilization of a huge membership (1 in every 4,000 Americans is an InfraGard member) that contributes private sector, industry-specific expertise to infrastructure and national security. With extensive background at the Federal Bureau of Investigation, Ms. O'Connell exemplifies the partnership that she leads. Since InfraGard's inception 25 years ago, the critical infrastructure landscape has dramatically changed. Each critical infrastructure sector is significantly more complex than was the case then. And 9/11, which occurred 5 years after InfraGard formation, heralded a period of rapid growth in the types and frequency of critical infrastructure threats. She was interviewed by JCIP Editor-in-Chief Richard Krieg in May, 2022.

Krieg InfraGard is a partnership between the Federal Bureau of Investigation and members of the private sector for the protection of U.S. critical infrastructure. The InfraGard program provides a vehicle for seamless public-private collaboration with government that expedites the timely exchange of information and promotes mutual learning opportunities relevant to the protection of critical infrastructure. Could you describe the organization's history and overall priorities?

O'Connell The InfraGard program celebrated its 25th anniversary last year and today represents the FBI's largest public/private partnership with over 80,000 members nationwide. The program's beginnings date back to

doi: 10.18278/jcip.3.1.2

1996, when the FBI's Cleveland Field Office engaged experts from private industry for a cybercrime investigation. But in the 25 years, and especially since the events of 9/11, it's been proven that by working together, the FBI and the American business community can multiply their respective efforts to mitigate acts of crime and terrorism.

Eighty-five percent of U.S. critical infrastructure is owned by the private sector, which is why it's so beneficial for the FBI to engage with the American business community. The InfraGard program takes an all threats, all-hazards approach to defending our nation's most critical assets, with a focus on the 16 critical infrastructure sectors established by Presidential Policy Directive 21 (PPD-21). It is our goal to align with the FBI's threat priorities, including terrorism, cybercrime, insider threats, violent crime, fraud and much more.

Krieg You served as an FBI Special Agent for 25 years. How did your experience with the Bureau help shape your perspective as President of InfraGard National Members Alliance (INMA)?

O'Connell My career as an FBI special agent was one of the most meaningful and rewarding experiences of my life. I had the privilege of working alongside the most dedicated men and women in the world. Working for the FBI, and in law enforcement in general, absolutely shapes my perspective as President of InfraGard National Members Alliance. Our job every day was to investigate and bring justice to those who would do harm to our country or the American people. In my daily work, I often saw the worst of humanity, from the types of crimes being committed to the impacts on the victims.

I also worked specifically on the InfraGard program while assigned to the FBI Los Angeles Field Office as a Private Sector Coordinator. Private Sector Coordinators are responsible for maintaining an understanding of the FBI's engagement with private industry at the field office level and connecting them with the right FBI personnel to address whatever challenges they are facing. All of these experiences strengthened my resolve to continue being part of the solution even after I retired from the FBI. I am a very proud American with a lot of love for this country, and InfraGard is an opportunity to continue giving back to a nation that's given so much to me.

Krieg With the FBI's interest in cyber counterterrorism, counterintelligence and so on - how does outside collaboration help?

O'Connell Since the majority of America's national security and economic infrastructure rests within the business community, invariably that's where you'll find many of the threats. If you look at some high-profile cyber-attacks and insider threat cases in recent history, the targets are often private sector companies. They hold the key to our nation's innovation and prosperity, and bad actors realize this. Safety and security must be a shared responsibility between private industry and law enforcement if we are going to stay ahead of the threat.

The InfraGard program is such a powerful vehicle because it promotes ongoing dialogue and timely communication between its members and the FBI. This two-way exchange of information equips InfraGard members with the knowledge, information, and resources to protect their respective organizations - while the FBI benefits from private sector engagement, insight and expertise that can help prevent terrorism, cybercrime, espionage and more.

Krieg Let's turn to the organization itself. How is InfraGard structured? And how does the organizational structure help in building security and resiliency across each critical infrastructure sector?

O'Connell The private sector component of the InfraGard program is represented by InfraGard National Members Alliance, an FBI-affiliated independent nonprofit organization. INMA is comprised of 77 localized non-profit organizations called InfraGard Members Alliances (IMAs), and we represent the IMAs in relations with the FBI.

Each of the 77 local IMAs is affiliated with one of the FBI's 56 U.S. field offices, addressing the threats in their respective localities from coast-to-coast and border-to-border. This is important because the IMAs possess local and regional expertise yet remain a vital piece of the larger national security picture. InfraGard National Members Alliance, with our national focus, and the InfraGard Members Alliances, with their local focus, provide a complementary approach to strengthening safety, security, and resiliency across America.

InfraGard National Members Alliance also addresses sector-specific security with two of our flagship programs: the National Sector Security and Resiliency Program (NSSRP) and the National Cross-Sector Council Program (NCSCP). The NSSRP provides a vertical approach, contributing to the InfraGard mission through the creation and sustainment of a "network-of-networks" that fosters collaboration and information sharing among owners and operators of critical infra-

structure within individual sectors. Led by Program Chair Dan Honore and a cadre of National Sector Chiefs, the NSSRP addresses the need for experts and intelligence for sector-specific activities.

Knowing there are many sector interdependencies and interoperabilities, the NCSCP provides a horizontal approach by addressing security threats and impacts that cross two or more critical infrastructure sectors. The NCSCP is led Program Chair Mary Lasky and seven National Cross-Sector Council chairpersons, providing the timely exchange of cross-sector specific information.

At the local level, many of the InfraGard Members Alliances have also built Sector Chief programs or Cross-Sector Councils to meet security and resiliency needs in their areas of responsibility.

Krieg Is it possible to say how your membership numbers break down by critical infrastructure sector?

O'Connell Currently, the Information Technology (IT) sector has the highest number of members in InfraGard, representing approximately 36 percent of our total membership. The Financial Services Sector represents about 10 percent of members, followed closely by Government Facilities (9 percent) and the Healthcare and Public Health Sectors (8 percent). Other prominent sectors include the Communications, Energy, Emergency Services, and Defense Industrial Base Sectors.

Krieg I'd like to focus on the organization's training and education functions – what are the principles that guide this work, how is it organized, and could you give examples of topics you are stressing?

O'Connell INMA strives to keep our fingers on the pulse of national threat priorities and provide content that's timely, relevant and valuable to our 80,000 plus members. National Infrastructure Security and Resilience U (NISRU) is our flagship eLearning platform, offering dozens of online courses, the Workshop Wednesdays series, and continuing education opportunities focused on critical infrastructure protection and resiliency. Through NISRU, we want to ensure that our members have the capabilities needed to meet the evolving landscape of critical infrastructure threats by providing comprehensive education, training, and workforce development for all 16 critical infrastructure sectors.

To provide an idea of the breadth of topics we cover, some recent NISRU offerings included "An Executive Approach to Cyber Risk Management", "Fundamentals of Homeland Security", and "Lessons Learned from Building the Intelligence Program at the NFL". Others include "Managing Risk in Supply Chain Software Applications", "Building an Effective Detection and Response Program", and "Tipping Point: Keys to Developing and Implementing a Comprehensive Violence Prevention Program."

Additionally, our National Sector Security and Resiliency Program (NSSRP) and National Cross-Sector Council Program (NCSCP) also produce webinars, events and information-sharing initiatives that are specific to individual sectors or cross two more sectors. For example, the National Disaster Resilience Council (NDRC), one of our Cross-Sector Councils, produces an annual summit. This year's edition in October will focus on the U.S. energy infrastructure and preparation for attacks and destructive natural events causing long-term power outages.

At the local level, InfraGard Members Alliances also produce numerous training and education programs that are customized to the security landscapes in their region. Their affiliations with local FBI Field Offices are vital in this regard, enabling the FBI to provide input and subject matter expertise pertaining to local threat priorities.

Krieg Given mounting concerns about cyber-attacks, what specific roles does InfraGard play to address that threat?

O'Connell Of the 16 critical infrastructure sectors, some are truly unique because of the enabling function they serve across all other sectors. The Information Technology Sector is one of them. America has become almost completely cyber-reliant, which has created our greatest Achilles heel. Cyber criminals, whether motivated by money or ideology, know this as well. That's why cyber represents the new battlefield.

InfraGard is based on collaboration, education, and information sharing, and this certainly holds true for addressing the cyber threat. Through our national programs, we work to provide educational webinars, workshops and courses on cyber threats and cybersecurity. Our FBI partners also collaborate with us to provide presentations and trainings, and we are very grateful for their insights and expertise. At the local level, InfraGard Members Alliances across the coun-

try are also sounding the alarm with cybersecurity-focused programs and events.

InfraGard members also gain access to the secure InfraGard Portal, which features the latest FBI intelligence, along with FBI and other government agency threat advisories, intelligence bulletins, vulnerability assessments and more.

Krieg At the time of this interview, the war in Ukraine looms large in the national mindset. Are there lessons for U.S. critical infrastructure resilience in that war?

O'Connell Initial reports indicate that Russia mounted several significant cyberattacks on Ukraine during the early phases of its offensive operations. Recent reports by Ukrainian officials and Microsoft have shown that most successes were of little strategic value to the Russian campaign. In fact, Ukrainian defenders were able to intercept an attack on the country's power grid - one that could have had significant consequences had it succeeded. The owners and operators of the U.S. critical infrastructure, across all sectors, should look at lessons learned from this conflict and prepare their own defensive strategies to counter recently demonstrated Russian tactics. Additionally, they should not believe that the worst is over. Experts agree that Russia has not unleashed its full cyber capability. CI owners and operators in the U.S. should seek out the latest information from sources such as CISA, and the FBI, as well as their software and systems integration providers. Information sharing between the public and private sector as well as private to private sectors will continue to be key to our collective defense against continued attacks from Russia, China, Iran - and other actors who are seeking to weaken our country through persistent cyberattacks.

Krieg As you look across the board in Infrastructure protection and resilience, what areas do you think most need attention in the next 5 years?

O'Connell One area needing attention would be to inspire our youth to rise to the challenge of becoming cyber experts. There are millions of high paying positions that sit vacant due to the low number of people with the requisite skills to fill them. We are at a critical point in this country and we all must work together to fill this void. InfraGard has a program called Cyber Camp in which we bring together young people of various ages to learn about cyber by inter-

acting with private sector entities and FBI Agents in an interesting way. We have them work through challenges in both a business and law enforcement environment and get them excited about a career in cyber. Through problem solving together, participants also enjoy learning about teamwork.

We are also focused on the threat that China presents in every aspect of critical infrastructure—from supply chain issues to theft of intellectual property, to the deep entanglement of our respective economies. These issues represent a multi-pronged attack on our country and cause staggering financial damages to our businesses. The FBI Office of Private Sector created a 30-minute movie that provides context for this threat (note: the referenced video is footnoted below).[1]

Another focal point is the safety and security of our citizens, especially our most vulnerable, so school safety is a priority. Through our trainings mentioned above, and our associations with the nation's 80 strategically located fusion centers, we provide a holistic approach to school safety, including Security Assessments and recommendations. Many of the tools we provide can be used across all sectors. We provide Open-Source Intelligence (OSINT) training to teach our members how to identify red flags, and address threats, while providing clear instruction on how and where to report tips and leads. These things combined raise the overall security posture of the entity, thereby increasing safety.

Raising money for these programs is also a priority and can be done either as a direct donation or a sponsorship. We invite people to be part of the solution, and all donations are tax deductible (note: the referenced site is footnoted below).[2]

Krieg Finally, how would a subject matter expert involved in critical infrastructure—whether it be as a business executive, professional, law enforcement, military, attorney, etc.—join InfraGard, and what opportunities exist for participation?

O'Connell Joining InfraGard is one of the best opportunities to take an active role in strengthening the safety and security of your hometown—where it all starts—and working alongside your fellow Americans to help build a safe, secure, and resilient nation.

Membership is free. Applicants must be U.S. citizens who are employed or formerly employed within critical infrastructure for at least

1 https://www.youtube.com/watch?v=GdapE82GceA

2 https://inma.salsalabs.org/nonmemberdonate/index.html

three years. They must consent to a security risk assessment, which is unique to the InfraGard program and aims to create a higher level of trust among our membership. People who want to apply should visit www.infragard.org. On being accepted for membership, you'll join one of the local InfraGard Members Alliances and have access to their education and information sharing programs. For more information about InfraGard National Members Alliance, you can go to our web site at www.infragardnational.org.

The benefits of membership are vast and include but are not limited to 24/7 access to InfraGard's secure web portal; FBI and DHS threat advisories and alerts, intelligence bulletins, and analytical reports; unique networking opportunities; FBI and other government agency briefings and resources; virtual and in-person training and education events and programs produced by the FBI, INMA and InfraGard Members Alliances. And, as previously mentioned, eLearning courses and workshops presented by INMA's National Infrastructure Security and Resilience U (NISRU).

Most importantly, InfraGard members know they are truly making a difference where it matters. We want to create a safe and secure nation for all Americans—and the future generations that will inherit what we leave behind.