# InfraGard National Sector Program – Application for Subject Matter Experts (SME)

Dear InfraGard Member,

Critical Infrastructures are the enablers of our entire American way of life. Assuring their protection, security, operational resilience, and all condition preparedness, is the most fundamental of National and Homeland Security imperatives and vital to ensuring America's and its citizens' safety, security, quality of life and future.

Unfortunately, it is these Critical Infrastructures that are increasingly viewed as legitimate targets by an ever-growing array of global actors ranging from opportunists, criminals, hackers and hacktivists, to terrorists and Nation States.

To enhance timely, accurate and effective dissemination and exchange of information across all Critical Infrastructure sectors, the *InfraGard National* and *Federal Bureau of Investigation* (FBI) established the **National Sector Program** with the goal:

> *To protect, secure, and ensure the operational resilience of the nation's interdependent, globally and Internet reliant critical infrastructure(s) by providing comprehensive expertise to communities throughout the land to assist all FBI field offices in protecting, securing and ensuring critical infrastructure resilience and all- condition preparedness in their areas of operations.*

In this call for applications, InfraGard National is taking steps to expand it's a ***Critical Infrastructure Sector Councils*** (CISC), with key Subject Matter Experts (SMEs), around each of the following *National Sector Chiefs* (NSC).

1. Communications Sector;
2. Defense Industrial Base Sector;
3. Emergency Services Sector;
4. Energy Sector;
5. Financial Services Sector;
6. Food and Agriculture Sector; and
7. Transportation Sector;

Led by that sector's NSC, selected SMEs will serve to assist the NSC in the establishment and support of IMA Sector Programs, and to provide sector specific subject matter expertise to the FBI in support of their critical infrastructure protection efforts.

## I. Minimum Qualifications for Sector SME candidates:

*The following qualifications apply to SME candidates:*

1. Be an InfraGard member in good standing with your IMA.
2. Hold, at a minimum, a bachelor's degree in an area related to your sector; a Masters or PhD level degree preferred.

3. Have been actively working within the target sector five (5) years minimum (10,000 hours).
4. Demonstrate awareness of current trends and threats in the sector through active engagement with multiple sector relevant professional organizations.
5. Demonstrate expertise as an SME and/or important stakeholder with a broad understanding, experience, and knowledge of the sector with interest in critical infrastructure protection; this can be demonstrated in many ways:
    A. Written books/articles on area of expertise;
    B. Hold requisite licenses, certifications, and/or trainings needed for expertise;
    C. Testified in a court of law as a SME;
    D. Been acknowledged in the media as a SME;
    E. Hold a reputation in your field as a SME, and can provide multiple references acknowledging your expertise; or
    F. Otherwise demonstrated expertise at national or global reach.
6. Possess strong briefing and communication skills.
7. Demonstrate ability to build effective relationships within their sector, other sectors, other communities (such as intel/fusion centers, DHS Protective Security Advisors, or other public/regulatory agencies).
8. Able to meet time and activity commitments as described below:
    A. Time commitment (10-20 hours/month) to successfully discharge their duties;
    B. Ability to travel to Washington, DC (1-2 times/year) if needed, to meet with FBI executives or other SMEs;
    C. Willingness to review a limited amount of intelligence information, with the FBI, to assess threats within the sector; and
    D. Contribute regularly to the sector community collaboration forums on the FBI portal.
9. Already holds or is willing and eligible to apply for a SECRET level security clearance.

## II. Sector SME Responsibilities, Duties and Desired Expertise Requirements

*Provided below is a description of the responsibilities, duties, and specific expertise we are seeking for selection as **Sector SMEs**.*

1. Responsibilities:
    A. Responsible and accountable to their Sector NSC for accomplishment of below listed duties and responsibilities.
    B. Responsible to INMA and IMA leadership, and to the FBI to serve as a Subject Matter Expert (SME) for their Sector.

2. Duties:

   A. Maintain currency on all FBI Headquarters and IMA sourced Critical Infrastructure threats, concerns, and information requirements.

   B. Provide expertise, advice and assistance to the FBI, partners, and federal sector oversight agencies.

   C. Provide sector expertise, advice, and assistance to the InfraGard National Board, fellow NSCC members, Regional Representatives, and IMA Sector Programs.

   D. Share relevant, timely, accurate, and actionable information to and from the FBI via personal contact, InfraGard Portal, FBI IGCs and/or iGuardian.

   E. Contribute within your CISC to help build-out and sustain local IMA Sector Programs and to support FBI critical infrastructure protection priorities.

   F. Support community outreach for critical infrastructure awareness, training opportunities, conduct of exercises, and continuing professional education programs.

**III. Desired Expertise, by Sector:**

We are specifically looking for subject expertise in the following sectors and technology areas:

A. Communications Sector:

   1) Traditional Telecom experience (Minimum expectation, working knowledge of Wireline, POTs, Cellular, RF, SDN, ISDN).

   2) Communications Emergency Services specialties (e911, PSAP, FirstNet, NPSTC members, ENP Certified).

   3) Communications Security Specialties (NSTAC members, Adjunct NSTAC members, security related certifications with emphasis on commercial or military communications security (COMSEC)).

   4) Emerging Communications Technology Specialties (5G, Hosted Cloud Communications Systems, LiFi, ROIP, IOT, Voice Biometrics, artificial intelligence (AI) specific to communications interaction (i.e.: Google Duplex).

B. Defense Industrial Base Sector:

   1) Understand technology protection programs in Defense Industrial Base.

   2) Have knowledge of Defense R&D, specializing in at least one warfighting domain.

   3) Understand threats to nuclear propulsion or weapon systems supply chain/fielding.

   4) Understand COMSEC deployment and supply chain.

   5) Understand Defense Counterintelligence efforts and threat training tools.

   6) Understand Defense Medical System and supply chain.

   7) Understand Defense IT and Cyber R&D, and fielding infrastructures .

   8) Expert understanding of NISPOM and DSS programs.

9) Understand Defense and Intelligence Information Security and PII Requirements.

10) Understand Defense UAV/UAS and VTOL-UAS R&D and supply chain risk and threats

11) Understand Insider Threat Programs and training to counter it (Doug)

- FOCI Foreign Ownership Controlling Interest
- Security Education
- Security Clearance program to include Limited Access Authorizations (LAAs) requests for Non-U.S. Citizens
- Understand Cleared Defense Contractor program from hiring to termination.
- Defense Industrial Base Facility Security Program from FSOs to gaining and maintaining a Facility Clearance.

C. Emergency Services Sector:

1) Police and Sheriff's office operations
2) Fire, Rescue, and Emergency Operations
3) Search & Rescue
4) Hazmat handling and response operations
5) Emergency Medical Services and operations
6) Emergency Management Command and Control
7) Air Law Enforcement operations; as they pertain to the operation of Drones
8) Public Safety Emergency Communications; includes NG911
9) Private Sector Security operations
10) Public Works Operations; including roads, bridges, tunnels, airports, harbors, terminals, flood control

D. Energy Sector:

1) Understand threats to the energy industry.
2) Understand of technologies that support current and innovative deployment of products and solutions.
3) Demonstration of building partnerships and engagement in information sharing to protect critical energy infrastructure.
4) Deep knowledge of architecture, use, and operational support in energy sector operational and information technology.
5) Communications and protocol knowledge of SCADA and traditional networking, and how to use machine learning to monitor and protect.
6) Specialized knowledge of design and threats to any of the following:

- Fault Location Isolation and Supply Restoration (FLISR);

- Distributed Generation (DG);
- Distribution Management System (DMS);
- Distributed Energy Resource Management System (DERMS); and
- Automated Meter Reading (AMR).

7) Expertise of threat, protections, and security technologies (physical/cyber) required in any of the following:
   - Nuclear generation;
   - Pipeline operation;
   - Drilling operations;
   - Energy Security Operations;
   - Substation or Transmission or system protection operations; and
   - Fossil generation.

E. Financial Services Sector:

1) Significant experience in financial services , which may include banking, credit unions, finance, lending, insurance, securities, and non-bank financial services, including fintech. Preference to those with experience in US domestic and global financial services

2) Desired areas of expertise may include one or more of the following:
   - Financial services supervision and operation of federal banking and payments systems (federal banking or financial services oversight agencies, and/or relevant state supervisors and licensing requirements.
   - Consumer credit, processing, settlement, and payments systems.
   - Commercial, business, and merchant banking and credit services.
   - International Trade Finance
   - Financial services law, supervision, examination, regulation, and oversight (US and global)
   - Securities instruments, clearing, and exchanges.
   - Wealth management and trust services.
   - Insurance and reinsurance.
   - Fintech and non-bank financial services, including emerging trends in innovative financial products, such as blockchain, AI, cryptocurrencies, payments, and lending.

F. Food and Agriculture Sector:

1) Expertise in the production agriculture: livestock, fruit, vegetable, production crops (corn, soybean, wheat, cotton, etc.), fisheries-ocean, inshore, inland, and aquaculture, Greenhouse and controlled environmental growing sites
2) Understanding the risks and vulnerabilities of pre and post-harvest food production.
    - Chemical, Biological, Radiological, Nuclear & Explosives (CBRNE)
    - Food safety principles and practices, inspection, certifications
3) Transportation - pre and post-harvest
4) Warehouse, retail, distribution of food and agricultural products
5) Knowledge of crop production, feed manufacturing, warehousing, transportation and processing
6) Knowledge of regulatory agencies: USDA, FDA, EPA, NOAA, CDC, NOAA, WHO
7) Veterinary medicine, University Extension, AG trade association management
8) Knowledge of import/export operations and regulations
9) Laboratory/diagnostic expertise
10) Expertise in Hazard Analysis Critical Control Points (HACCP) and other Systems Management protocols
11) Knowledge of the pet, companion animal food industry
12) Knowledge of the Equine industry

G. Transportation Sector

1) Deep knowledge and expertise in one (or more) of the DHS subsectors, to include:
    - Aviation
    - Highway and Motor Carrier
    - Maritime
    - Mass Transit and Passenger Rail
    - Freight Rail
    - Pipeline Systems
    - Postal and Shipping
2) Transportation Sector resilience after a catastrophic disaster (with a focus on airports, maritime ports, rail lines, and highways);
3) Autonomous vehicles and vehicle telematics;
4) The impact of drone technology;

5) The use of Blockchain technology in emergency supply chain management; and

6) Intelligent Transportation Systems (Highway, Commercial Vehicle, Public Transportation and Emergency Services modes).

## IV. TERM OF OFFICE:

Sector SMEs will be appointed for a two-year term by the National Sector Program Manager (NSPM); reappointments or extensions are possible, and will be at the discretion of the NSPM and cognizant NSC.

## V. APPLICATION DIRECTIONS:

1. To apply for this position, you must submit:
   A. A recent resume;
   B. A two-page personal statement covering all of the points below:
      - Demographic information – full name, chapter, company, current title, and phone/email contact information;
      - Personal statement that describes the following
        - State the sector you wish to serve in as an SME;
        - Address all of the selection criteria listed in Sections I and III. above;
        - Describe why you are interested in serving as a sector SME;
        - Describe how you feel your skills and expertise can help InfraGard and the FBI protect critical infrastructure.
2. **Email your resume and personal statement** to cgeorgo@infragardnational.org

***Note: This solicitation will remain open until cancelled/modified.***