**INFRAGARD**

****

**National Sector Security and Resilience Program (NSSRP) Handbook**

**June 22, 2022**

*Version 2*

# Change Log

|  |  |  |  |
| --- | --- | --- | --- |
| Author | Date | Version | Nature of Change |
| Chuck Georgo | 20190330 | v0 | Initial draft of revised and renamed handbook |
| Chuck Georgo | 20190414 | v1 | Released revised handbook to InfraGard National website |
| Chuck Georgo | 20190416 | v1a | Minor update |
| Chuck Georgo | 20190424 | v1b | Incorporated InfraGard National Chairman edits |
| Chuck Georgo | 20191101 | V1c | Added AutoISAC to Appendix VII |
| Daniel Honore | 2021 | V2 | Added Program Manager responsibilities. Added Deputy NSC responsibilities Changed “Resiliency” to “Resilience” in program name. Updated term-limits for NSC and SME |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Table of Contents

[Acronyms and Abbreviations iv](#_Toc6153526)

[Executive Summary v](#_Toc6153527)

[I. INTRODUCTION 1](#_Toc6153528)

[1. Authorities 2](#_Toc6153529)

[2. FBI Office of the Private Sector (OPS) 2](#_Toc6153530)

[3. InfraGard National 2](#_Toc6153531)

[4. InfraGard National Sector Security and Resilience Program (NSSRP) 3](#_Toc6153532)

[5. InfraGard Members Alliance (IMA) SSRP 3](#_Toc6153533)

[II. Sector Security and Resilience Program Overview 5](#_Toc6153534)

[1. InfraGard NSSRP Purpose and Goals 5](#_Toc6153535)

[2. National Sector Chief Council (NSCC) 5](#_Toc6153536)

[3. National Subject Matter Experts (SME) 6](#_Toc6153537)

[III. IMA Sector Program Guidance 8](#_Toc6153538)

[1. Preparing to Establish a new IMA SSRP 8](#_Toc6153539)

[2. General Steps to Establishing an IMA SSRP 8](#_Toc6153540)

[3. Specific Advice for Building an IMA Sector Program 10](#_Toc6153541)

[4. Advice and Guidance for Operating and Sustaining an IMA Sector Program 13](#_Toc6153545)

[5. Advice and Guidance for Implementing Effective Information Sharing 14](#_Toc6153550)

[Appendix I – Critical Infrastructure Sectors 18](#_Toc6153555)

[Appendix II – RENS Implementation Support 24](#_Toc6153572)

[Appendix III – National Sector Chief Selection Process 26](#_Toc6153573)

[Appendix IV – IMA Sector Chief Selection, Employment, and Evaluation Tools 27](#_Toc6153574)

[Appendix V – IMA San Diego (Example) Sector Chief Selection/Lifecycle Process 30](#_Toc6153578)

[Appendix VI – IMA SSRP Sustainment Tools 32](#_Toc6153581)

[Appendix VII – ISACs/ISAOs 35](#_Toc6153586)

[Appendix VIII – Traffic Light Program Detailed Guidance 36](#_Toc6153587)

# Acronyms and Abbreviations

AIS Automation Information Sharing

AOR Area of Responsibility

BoD InfraGard National Board of Directors

CCISCP Cyber Information Sharing and Collaboration Program

CI ISE Critical Infrastructure Information Sharing Environment

CI Critical Infrastructure

CIP Critical Infrastructure Protection

CSA Cyber Security Advisor

DHS Department of Homeland Security

DIB Defense Industrial Base

DNSC Deputy National Sector Chief

ESF Emergency Support Function

FBI Federal Bureau of Investigation

FEMA Federal Emergency Management Agency

HSIN Homeland Security Information Network

HSIN-CI Homeland Security Information Network-Critical Infrastructure

IMA InfraGard Members Alliance

ISC IMA Sector Chief

ISAC Information Sharing and Analysis Center

ISAO Information Sharing and Analysis Organization

MOU Memorandum of Understanding

NCCIC National Cybersecurity and Communications Integration Center

NCSC National Communications Sector Council

NDA Non-Disclosure Agreement

NEMA National Emergency Management Association (NEMA)

NIST National Institute for Standards and Technology

NITSC National Information Technology Sector Council

NSC National Sector Chief

NSCC National Sector Chief Council

NSSRP National Sector Security and Resilience Program

OPS Office of the Private Sector

PCII Protected Critical Infrastructure Information Program

PSA Protective Security Advisor

PSC Private Sector Coordinator

RENS Recruitment, Education, Networking and Information Sharing

SAR Suspicious Activity Report

SC Sector Chief

TLP Traffic Light Protocol

US CERT United States Computer Emergency Response Team

USSS United States Secret Service

# Executive Summary

This handbook was prepared for the *InfraGard National Board of Directors (BoD)*, all *InfraGard Member Alliances* (IMAs), and InfraGard members to provide information and guidance for establishing and sustaining an effective *National* *Sector Security and Resilience Program* (NSSRP) at the National level and within all chartered IMAs.

This handbook provides guidance, advice, tools and templates to help Board Directors, IMA leadership, InfraGard members, and FBI Private Sector Coordinators (PSC) to establish, grow, sustain, and objectively measure the effectiveness of their InfraGard Sector Program.

The handbook is arranged into four sections and eight appendices; the contents of each is summarized below:

1. **Introduction** – Introduces the Infragard NSSRP, the organizations involved, and its purpose.
2. **NSSRP Overview** – Provides a description of the NSSRP, its purpose and construct, and the responsibilities for the *National Sector Chief Council* (NSCC) and individual *national sector councils[[1]](#footnote-2)*.
3. **IMA SSRP Program Guidance** – provides guidance and advice on the establishment and sustainment of local IMA SSRP elements, and on information sharing in support of SSRP program activities.
4. **NSSRP Sustainment Tools** – describes tools available to local IMAs to help build and sustain their local SSRP.

**Appendices** – Provides additional information on Critical Infrastructure (CI) Sectors, Recruitment, Education, Networking, and Information Sharing (RENS) implementation support, National Sector Chief (NSC) selection process, additional Sector Program Tools and Checklists, information sharing Traffic Light Program detailed guidance, links to Department of Homeland Security (DHS) Sector Specific Plans, and a list of current Sector ISACs/ISAOs.

# INTRODUCTION

Under the DHS, there are sixteen *CI Sectors*.[[2]](#footnote-3) Together, these sectors are the enablers of American life. Assuring their protection, security, operational resilience, 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, these Infrastructures are increasingly viewed as *legitimate targets* by an ever-growing array of global *actors* ranging from cyber criminals, hackers and hacktivists, to lone-wolf, domestic and international terrorists, as well as natural disasters. This requires an ‘All-Hazards approach. They also recognize America’s increasing reliance on the Internet creates a low risk/high-payoff “vector,” a *great equalizer* and in effect an emerging *single point of failure*.

InfraGard is a nation-wide partnership between the Federal Bureau of Investigation (FBI) and members from the private sector that create opportunities to collaborate, share and communicate information about a perceived or potential threat about a CI component, system, platform, device or manufacturer. Membership includes business executives, entrepreneurs, military personnel, government officials, physical and information security professionals, academia, and law enforcement.

InfraGard is implemented through the *InfraGard National* and IMAs (aka chapters) established in communities throughout the Nation. Together, they form a uniquely organized and knowledgeable sector and cross-sector network positioned to effectively and efficiently:

Foster the collaborative and bi-directional exchange of CI intelligence, information, and education;

Identify CI sectors and cross-sector threats, gaps, exploitable vulnerabilities; protection, security, resilience and preparedness issues and single points of failure;

Share community-based infrastructure information and performance requirements and challenges in meeting them, and

Provide a conduit to speed the implementation of CI protection, security, resilience and preparedness innovations

InfraGard provides the means to ensure accurate and actionable local/regional CI threat, risk and vulnerability awareness and continuous improvement in CI operations.

**InfraGard Mission:**

The mission of the InfraGard Program is to foster collaboration, education and information exchange to enhance America’s ability to comprehensively address and eliminate threats to its critical infrastructure through a robust private-public partnership. InfraGard promotes ongoing dialogue and timely communication between members and the FBI.

InfraGard brings together representatives from the private and public sectors to help protect and promote the security and resilience of our Nation’s critical infrastructure - both virtual and physical - from attacks by terrorists and criminals and disasters. The Federal Bureau of Investigation, Office of the Private Sector (OPS), and InfraGard National BoD and Officers manage the InfraGard program at the National level.

## Authorities

InfraGard Program activities support many National directives; two primary directives include:

* Presidential Policy Directive-21 (PPD-21) “Critical Infrastructure Security and Resilience” and Executive Order 13636 (EO 13636) “Improving Critical Infrastructure Cybersecurity,” direct the Federal Government to coordinate and work with the private sector to share timely information to make the Nation’s CI more secure and operationally resilient.
* Homeland Security Presidential Directive-7 (HSPD-7), “Critical Infrastructure Identification, Prioritization and Protection”, specifies the FBI is responsible for reduction of domestic terrorist threats, as well as investigation and prosecution of actual or attempted terrorist attacks on, sabotage of, or disruptions of CI and key resources.

The InfraGard NSSRP works with the FBI and other Federal agency partners to build trusting relationships, conduct education and training, and to share information with the public and private sector entities that own or operate America’s CI.

## FBI Office of the Private Sector (OPS)

The mission of the FBI is to “protect and defend the United States against terrorist and foreign intelligence threats, to uphold and enforce the criminal laws of the United States and to provide leadership and criminal justice services to federal, state, municipal and National agencies and partners.”

The FBI works with both government and private sector partners every day and at every level – local, state, tribal, National and international. InfraGard is an example of this comprehensive engagement. In some cases, these partnerships directly support investigations and operations.

In other cases, they enable mutually beneficial information sharing and exchange that help the FBI to better understand emerging threats, exploitable vulnerabilities, infrastructure performance shortfalls, and foster crime prevention, and counterespionage initiatives.

OPS develops and supports partnerships between InfraGard and the FBI and other private sector, academic, and public entities, to support execution of National Security Strategy and supporting FBI priority investigative programs.

## InfraGard National Members Alliance (InfraGard National)

The InfraGard National is the National Governing Board the Executive Director and staff for IMAs throughout the Nation. The InfraGard National bylaws state the purpose and primary objective of the InfraGard National is to “increase the security of our National Infrastructure through ongoing exchanges of information and through outreach and similar efforts to increase awareness of infrastructure protection security and resilience issues in communities throughout America."

The InfraGard National promotes the InfraGard mission of protecting and supporting the security and resilience of the Nation’s interdependent cyber and physical CI by providing communication, coordination, resources, education, expertise, and governance to IMAs, their members, communities and infrastructure stakeholders throughout the Nation. The InfraGard National mission is to execute the InfraGard mission through supporting partnerships and opportunities with the private sector and all government agencies directly and through local IMAs.

## InfraGard National Sector Security and Resilience Program (NSSRP)

The NSSRP was originally conceived as the Sector Chief (SC) Program within the Kentucky IMA in 2003. The success of the program in Kentucky led to the expansion of the program throughout InfraGard chapters nationwide starting in 2012.

The program contributes to overall InfraGard mission through the creation and sustainment of a “network-of-networks” to foster collaboration and information sharing among and between owners, operators, and participants of CI within individual sectors.

Led by a NSSRP Program Manager and the InfraGard NSCC, the NSSRP provides leadership, guidance, and support to IMA Chapters, helping them to develop and sustain an effective SSRP within their Chapter.

A successful NSSRP, at either the national or IMA levels, will engage in four key activities – **Recruitment, Education, Networking, and Information Sharing (referred to as RENS):**

* **RECRUITMENT** – Recruitment of representative CI owners, operators, and participants pertinent to the local IMA;
* **EDUCATION** – Provision of education and training that meets the needs of CI owners, operators, and participants;
* **NETWORKING** – Enablement of intra-sector and inter-sector networking opportunities for CI owners, operators and participants; and
* **INFORMATION SHARING** – Timely, accurate, and actionable two-way information sharing.

## InfraGard Members Alliance (IMA) SSRP

Each IMA should establish an SSRP that represents the significant sectors present within their Chapter’s area of responsibility as it aligns with their area of responsibility (AOR).

A well implemented IMA SSRP helps to provide direct focus and leadership around the four RENS activities described in paragraph 4 above.

* ***Appendix II*** *provides very detailed questions IMA leadership can use to implement and evaluate RENS activities within their area of responsibility*



These activities in conjunction with the FBI Field Office will help ensure the IMA is engaging the right CI owners and operators, providing them with effective education and networking opportunities, and conducting timely and effective dissemination and exchange of sector-specific and cross-sector information needed to protect, secure, and ensure the operational resilience of the capabilities and services provided by CI within those sectors.

Each IMA SSRP will be led by an IMA SSRP Coordinator, selected by the IMA leadership. The SSRP Coordinator will be responsible for the selection of a SC for each of the sectors selected for that IMA. The SSRP Coordinator and individual SCs will work collaboratively, with the NSCC, local partners, and others to meet the objectives of the InfraGard NSSRP.

For IMA leadership, SSRP Coordinators, and IMA members, partners and collaborators, here’s a list of benefits that an effective SSRP can provide; use this list to help develop, enhance or sustain your local program.

* Keeps everyone informed on newly identified or prevalent threats in the specific sector of interest;
* Communicates and share sector security and resilience best practices and guidelines;
* Makes available forums to discuss common threat/vulnerability issues within specific sector;
* Provides multiple channels of timely, relative, actionable information;
* Provides a resource for speakers on topics relevant to sector security and resilience;
* Increases collaboration and connectivity between sector CI operators, and security and resilience partners and collaborators;
* Promotes sharing of ideas and information, serve as a network source for key leadership and subject matter experts between private partners and federal, state and municipal agencies/entities;
* Provides resources for education and training opportunities;
* Serves as platform to engage government leadership to discuss current issues and future sector security and resilience concerns;
* Enables the sharing of sector/cross-sector security and resilience checklists, guidelines, and tools;
* Provides increased security awareness programs for the business community sector;
* Gain insight to what others in specific sectors view as current and future challenges to sector security and resilience, and potential mitigations; and
* Enables the sharing of known attack vectors and solutions for hardening defenses.
* Provides an ‘All-Hazards’ approach to security and resilience.

# National Sector Security and Resilience Program Overview

## InfraGard NSSRP Purpose and Goals

The purpose of the InfraGard NSSRP is to enhance timely, accurate and effective dissemination and exchange of sector and cross-sector specific information to protect, secure and ensure the operational resilience of the nation’s interdependent, global, and Internet reliant CI.

Goals of the InfraGard NSSRP include:

* Build and maintain an integrated national cadre of InfraGard CI sector subject matter experts (SME), innovators, advocates and other important CI stakeholders at the InfraGard National and in every IMA;
* Serve as a liaison with other Federal agencies and organizations related to the CI Sectors on a National basis to assure the exchange of information and tools to assist the IMA SCs;
* Identify and adopt Sector Program best practices;
* Align the scope of the Sector Program and individual IMA Sector Programs with the priorities of FBI Headquarters and each FBI field office respectively;
* Develop the ability to share sector and cross-sector expertise, knowledge and experience at and between the National and chapter levels;
* Ensure continuous, objectively measurable, improvement in business, community and national CI protection, security, disaster, operational resilience and preparedness.

## National Sector Chief Council (NSCC)

The InfraGard National BoD established the NSCC to help build and sustain a cadre of NSCs and SMEs who will support the establishment, growth and sustainment of IMA SSRP efforts. Led by an InfraGard National BoD appointed NSSRP Program Manager, the NSCC interacts with IMA appointed SCs for the development of IMA SSRP efforts and with the FBI InfraGard Program Manager to satisfy their subject matter expertise needs.

## NSSRP Program Manager

The NSSRP Program Manager is appointed by and serves at the pleasure of the InfraGard National BoD. Program Manager responsibilities include:

* Provides leadership, guidance, and support to IMA Chapters, helping them to develop and sustain an effective SSRP within their Chapter.
* Serve as the National Sector Security and Resilience Program leader, spokesperson and Subject Matter Expert in all InfraGard National meetings, conferences, and annual Congress.
* Recruit National Sector Chiefs (NSC) and Subject Matter Experts (SME) who will support the establishment, growth and sustainment of IMA SSRP efforts, within their respective sector.
* Assist NSCs with recruitment and retention of SMEs within their sector.
* Initiate and participate in InfraGard projects and initiatives at the national and regional levels.
* Develop an annual program plan and budget for the NSSRP.
* Provide to the InfraGard National BoD monthly reports of planned activities, accomplishments, and achievements of the NSSRP.
* Continually evaluate and Support the sharing of relevant, timely, accurate, and actionable information to the FBI via personal contact, [InfraGard Portal](https://www.infragard.org/), FBI PSC, [iGuardian](https://www.fbi.gov/resources/law-enforcement/iguardian), and to the Federal agency (or agencies) with oversight responsibility for their corresponding sector or state fusion centers.

The NSSRP Program Manager will work with the InfraGard National BoD, National Sector Chiefs, Subject Matter Experts, Regional Representatives, and IMA leadership in the performance of these responsibilities.

## National Sector Chief (NSC)

NSCs are appointed to two-year terms through a competitive selection process led by the NSSRP Program Manager.[[3]](#footnote-4) Appointments resulting from this process are ratified by the NSSRP Program Manager BoD. NSC responsibilities include:[[4]](#footnote-5)

* Serve as the National leader, spokesperson and Subject Matter Expert representative for their Sector in all InfraGard National meetings, conferences, and annual Congress.
* Guide IMA SC’s in the development, implementation and operation of their program.

* ***Appendix III*** *provides a description of the National Sector Chief Selection and appointment Process.*



* Support other National and IMA SCs in the sharing of relevant, timely, accurate, and actionable information to the FBI via personal contact, [InfraGard Portal](https://www.infragard.org/), FBI PSC, [iGuardian](https://www.fbi.gov/resources/law-enforcement/iguardian), and to the Federal agency (or agencies) with oversight responsibility for their corresponding sector or state fusion centers.
* Interact regularly with other National and IMA SCs, and members regarding;
  + Two-way information exchange and community outreach efforts;
  + Development of CI education opportunities;
  + Discovery of CI protection, security and resilience innovations;
  + Identification and resolution of CI issues (e.g. single points of weakness and/or failure); and
  + Sharing of community CI performance requirements that help ensure national program consistency.
* Recruit Subject Matter Experts (SME) who will support the establishment, growth and sustainment of IMA SSRP efforts, within their respective sector.
* Assist IMAs with recruitment and retention of CI owners, operators, and participants within their sector.
* Engage with IMA SCs to accelerate community outreach for CI awareness, training opportunities, exercises, and continuing professional education programs.
* Initiate or participate in InfraGard projects and initiatives at the regional or national levels.
* Develop an annual program plan and budget for each National Sector.
* Provide monthly reports of planned activities, accomplishments, and achievements.

NSCs appointed to the NSCC will work with the InfraGard National BoD, NSSRP Program Manager, Regional Representatives, and IMA leadership in the performance of these responsibilities.

## Deputy National Sector Chief (DNSC)

Deputy National Sector Chief is appointed by the CI sector National Sector Chief. The responsibilities of a DNSC include the responsibilities of an SME in addition to the following:

* Assist the NSC in execution of NSSRP mission.
* Support the NSC in executing the responsibilities of the NSC role.
* Attend NSCC meetings.

## National Subject Matter Experts (SME)

Each NSC on the NSCC will recruit Subject Matter Experts (SME) who will support the establishment, growth and sustainment of IMA SSRP efforts, within their respective sector. These SMEs will also be available to the FBI InfraGard Program Manager to help satisfy the need for subject matter expertise that FBI Headquarters or Field Offices require in support of the CI protection mission (Criminal, Cyber, Terrorism, Counterintelligence and/or WMD).

SMEs are appointed through a competitive selection process led by the CI sector NSC and the NSSRP Program Manager; this process is similar to the NSC selection process described in Appendix III.[[5]](#footnote-6) Appointments resulting from this process are ratified by the CI sector NSC and NSSRP Program Manager. There is no term of office for SMEs but continual evaluation of engagement and contribution to the success of the NSSRP ensures each SME provides value to the program.

SME responsibilities include:

* Serve as spokesperson for their Sector in meetings, conferences, or annual Congress, as appropriate.
* Maintain awareness of all FBI Headquarters and IMA sourced CI threats, concerns, and information requirements.
* Provide expertise, advice and assistance to the FBI, partners, and federal sector oversight agencies.
* Provide sector expertise, advice, and assistance to the InfraGard National Board, fellow NSCC members, Regional Representatives, and IMA Sector Programs.
* Share relevant, timely, accurate, and actionable information to and from the FBI via personal contact, InfraGard Portal, FBI PSC and/or iGuardian and state fusion centers.
* Contribute within your respective national sector council to help local IMAs develop or enhance their local SSRP program, and to support any FBI or other governmental agency need for your expertise in their CI protection efforts.
* Support community outreach for CI awareness, training opportunities, conduct of exercises, and continuing professional education programs.

# IMA Sector Program Guidance

This section of the handbook provides guidance, tools, templates, and advice for IMA leadership to establish, sustain, and support an SSRP within their IMA Chapter.

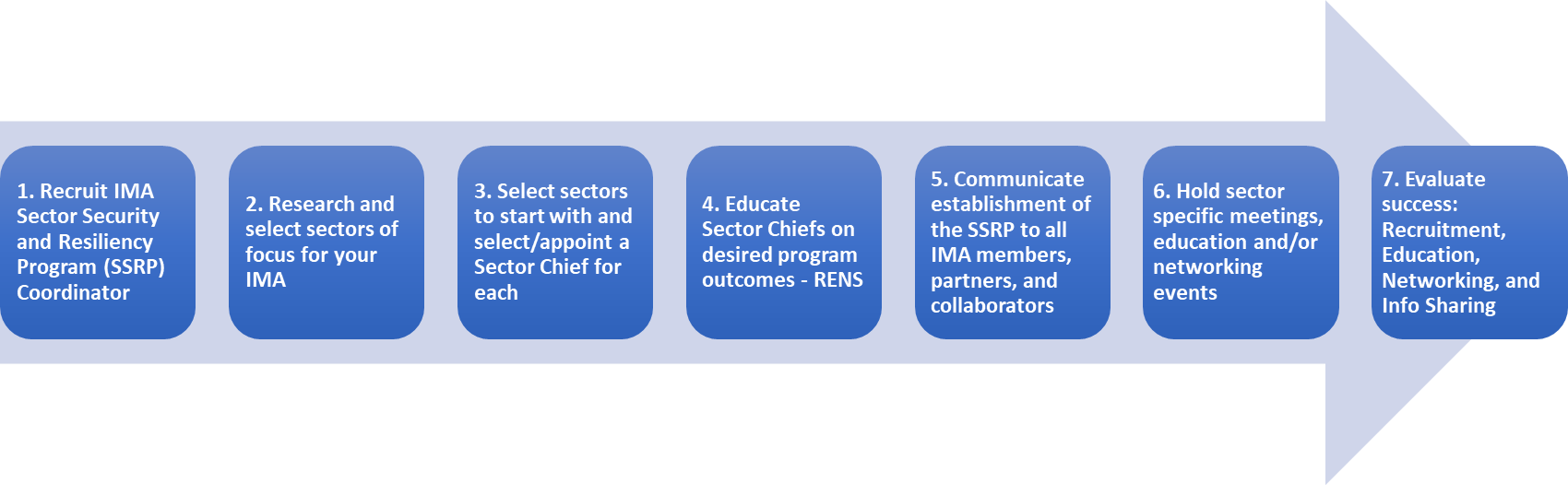
## Preparing to Establish a new IMA SSRP

Before starting an SSRP within your IMA, some advance research is required to prepare your IMA. This research will assist you to gather information that will help to identify the sectors to start with, to identify IMA members who can help with getting your SSRP started, and to identify key partners who will support the newly established SSRP. Here are three areas of research to consider:

* Gain knowledge of the CI environment in the IMA’s area of responsibility, in conjunction with your FBI PSC, DHS Protective Security Advisor (PSA), and Cyber Security Advisor (CSA), identify the primary CIs in your AOR. Each IMA will have a unique CI profile, both in relevant sectors and in sector priorities. Some examples include:
  + San Diego is a large tourist destination, therefore the Commercial Services Sector (theme parks, casinos, hotels, shopping malls, sports venues, mass gatherings, etc. are critical areas for emphasis).
  + Gulf Coast IMAs are in the nation’s primary production area for refined fuels and also face ongoing weather-related threats making Energy and Emergency Services Sectors particularly vulnerable and critical.
  + The National Capitol Region holds headquarters of all three branches of government, and national security, homeland security, and intelligence agencies, and so threats to the Defense Industrial Base and Government Facilities would be of significant emphasis.
* Become familiar with the DHS Sector Specific Plans for the sectors you select, published at this website <https://www.dhs.gov/2015-sector-specific-plans>.
* Identify IMA members who can help you start the SSRP within your IMA – leaders who have emerged or volunteered to take on additional responsibilities. Sector leadership requires more than just sector-specific expertise, it includes strong people skills and the ability to motivate, organize and lead.
* Develop partnerships with key IMA partners (in coordination with IMA leadership): FBI Coordinator, DHS PSA, and regional/state fusion center. Without key partner involvement and assistance with CI prioritization, any Sector Chief program will face significant hurdles.

## General Steps to Establishing an IMA SSRP

This section provides a starting point for IMA leadership to start their SSRP. The general process for establishing a SSRP is illustrated in the flowchart below; IMA leadership should tailor this process to fit their specific needs.



More detailed steps are included below.

1. IMA leadership should canvas members to identify a volunteer to serve as the IMA SSRP Coordinator; be sure that IMA leadership formally appoints the individual to the position.
2. The appointed SSRP Coordinator needs to research the CI sectors represented in your IMA and build an inventory of members, by sector, to determine which sectors are most significant within your IMA.
3. From this inventory, IMA leadership and the SSRP Coordinator should work collaboratively to select one or two sectors to begin with in building the IMA SSRP, and recruit and formally appoint a SC for each.
4. IMA leadership and the SSRP Coordinator should educate the newly selected SCs on the purpose of the program and performance expectations and how RENS is relevant as an implementation and evaluation tool; the more specific the expectations, the more likely the SSRP will be a success.
5. Prepare an announcement to IMA membership, announcing the establishment of the IMA SSRP, the names of the sectors selected to start the program, and the names of the newly appointed SCs.
6. For each newly appointed SC, have them schedule and invite IMA members and partners to a kickoff meeting for their respective sector. At this meeting, each SC should facilitate development of a plan of action for future meetings, educational workshops, and other information sharing activities to advance the goals of the SSRP.
7. Final step, IMA leadership and the SSRP should establish some basic measures of effectiveness that IMA leadership and the SSRP can use to evaluate the effectiveness of their IMA SSRP.

* **Recruitment measure** – have we recruited representative owners, operators, and participants from all CI organizations present in our chapters area of responsibility?
* **Education measure** – Are we presenting/offering educational opportunities that address the most pressing threats/vulnerabilities as skills enhancement within that sector?
* **Networking measure** – Do we provide opportunities for owners/operators and participants within a specific sector to network and share information with one another?
* **Information sharing measure** – To what extent is the FBI and DHS or sector specific agencies sharing specific, relevant threat information with owners, operators, and participants in each sector? Are owners and operators within each sector actively sharing information back with the FBI?

Additional suggestions:

* At the conclusion of the kickoff meeting, prepare an announcement to IMA members to let them know the results of the meeting, agreed upon goals and objectives for that sector, and invite additional participation in future SSRP activities.
* Once the first one or two IMA sector-specific programs are established, expand the SSRP to additional sectors, as volunteers are available.
* Work with the FBI PSC to ensure that your IMA SCs name and contact information is loaded into the FBI Portal.

## Specific Advice for Building an IMA SSRP

This section will provide more detailed guidance and advice for *building* an IMA Sector Program.

### Selecting a Sector Chief

To be effective a **Sector Chief MUST be a member of the IMA he/she is a Sector Chief for and reside in/near the IMA’s Area of Responsibility**. The SC needs to be able to visit with local FBI field office, stakeholders, attend member meetings and participate in local events.

A good SC is first of all a good leader with above average people skills. But expecting one person to organize and lead a sector, especially a complex sector like Commercial Services, Healthcare or Transportation is asking a lot of our volunteer IMA folks, most of whom have “day jobs”.

One best practice that seems to work is to engage SCs in each Sector and sub-sectors so that one person does not shoulder the entire responsibility for his or her sector. For example:

*In one IMA Education subsector, there are three Higher Education co-SCs and one K-12 SC. This is particularly relevant for those sectors like Commercial Facilities that has eight sub-sectors. You should have a SC for each sub-sector.*

*Because of the disparity in target audience sizes (greater number of school districts and schools relative to universities and colleges in the region), another K-12 co-SC is being added to this team.*

*Having multiple co-SCs puts the emphasis on working together effectively as a team for recruiting, planning, educational outreach to the IMA and intra-sector and cross-sector events. As the SSRP grows in size and in the use of collaborative tools for information sharing, good teamwork becomes even more important.*

Local IMAs are free to set their own term of office for local SCs; however, it is recommended that appointment terms are codified in a formal appointment letter.

Here’s a summary of optimal SC qualities:

* Motivated leaders within the IMA membership with strong communication skills.
* Subject matter experts possessing experience in conducting CI protection, security and resilience operations within their sectors.
* Currently employed within the sector they represent.
* Important stakeholders who have a proven understanding and knowledge of their sectors and its interdependencies.
* Recognized voice of that sector’s community, with access to networking opportunities and the ability to build effective relationships within their infrastructure sector.
* Has the time to commit to the position.

### Sector Chief responsibilities

Here is a suggested list of SC responsibilities; adjust these as needed to fit the needs of each sector within your IMA SSRP.

#### Must be able to identify and provide external subject matter expertise:

* Must have a strong public presence representing a CI sector.
* Be able to speak on CI sector and cross-sector topics, challenges and their solutions.
* Serve as an outreach and information exchange advocate and InfraGard resource for their communities.

#### Must be willing to perform as the IMA Point of Contact (POC) for sector related information and issues to oversee the following.

* Receipt of sector and cross-sector communications from the FBI and its interagency partners.
* Soliciting, collection and participation in sector and cross-sector intelligence and information needs development.
* Dissemination of sector and cross-sector information and information needs to IMA members, FBI InfraGard Coordinators, and other agencies as agreed.
* Sharing of sector and cross-sector issues, information and performance requirements with other SCs.

#### Must promote collaboration within the sector and those reliant upon it with InfraGard members and non-members.

* Assist in IMA Chapter member recruitment, involvement and retention.
* Assist with IMA Chapter awareness, education and training efforts throughout their respective communities.
* Create, conduct and/or attend community-focused infrastructure sector and cross-sector specific meetings and exercises.
* Actively engage InfraGard members to facilitate CI awareness and information exchange and the discovery and implementation of CI protection, security, resilience and preparedness innovations.

#### Actively pursue working relationships with DHS PSA and CSA, Fusion Centers, State and Local agencies (particularly State and county Emergency Management Departments), and potentially high-consequence producing entities throughout the IMA’s area of operations.

* ***Appendix IV*** *provides additional information and advice for selecting, employing and evaluating IMA SCs.*
* ***Appendix V*** *describes the SC selection process for the San Diego IMA; use this to shape a process for your IMA.*



### Engaging IMA SCs

Although some IMA SCs might be self-starters, the norm is that most can be overwhelmed by their IMA’s expectations. You may go for months without hearing from some of your SCs at which point intervention is required. Here are some ideas that might get these SCs moving towards greater engagement:

* + Encourage SCs to provide an educational program at an IMA Chapter meeting – e.g. describe what their sector looks like in that region and some security challenges that need to be met.
  + Encourage multiple SCs to host a cross-sector event that for example might include energy, transportation, water and emergency services to discuss sector interdependencies.
  + Make sure all SCs meet and use their DHS PSA. PSA’s have access to a variety of excellent CI training materials.
  + Engage SCs in local and regional exercise planning.
  + Ensure that particularly effective SCs receive public recognition for their efforts. Use InfraGard National’s SC of the Year Award where warranted.
  + Have model SCs mentor those who have more issues getting started.

## Advice and Guidance for Operating and Sustaining an IMA Sector Program

Operating an effective SC program requires several ongoing activities: new member recruitment, member education, member networking and developing an effective and user-friendly information sharing environment. Each of these elements will be described below.

### Member recruitment

Member recruitment is a key starting activity for not only a new SC program but also for program sustainment. Each SC will need to recruit active members within their sector to help with program development and other sector-related activities.

### Member education

Member education has at least two dimensions: educating sector members on threats and mitigation topics relevant to their sector and educating the general IMA membership on the relevance of their sector to the IMA’s region.   
  
For example, an IMA Education Subsector (Government Facilities Sector) recently had a sector meeting on issues surrounding student protests on campus and an IMA Healthcare Sector conducted a presentation on infectious diseases that impacted a recent arrival of large numbers of Haitian refugees in the IMA’s AOR. Another example involved the Faith-Based Subsector (Commercial Services Sector) organizing an annual Church Safety Conference, the only known such conference in the nation.

### Member networking

An important area of sector interaction is to schedule networking events, either as part of a general IMA meeting or as a sector-specific activity. The key here is to give infrastructure owners and operators the opportunity to talk with each other about the challenges faced and opportunities for enhancing protection of assets in their respective sector. One example might be a tour of a geographically-relevant critical facility within that sector. Collaboration with county emergency managers and first responders is another important networking opportunity.

### Information Sharing

Finally, and arguably the most valuable component of the InfraGard program, is the creation and sustainment of robust two-way information sharing; between members, between members and the FBI, and between the FBI/DHS and sector members. Specific focus on this element is provided in Section 5 below.

* ***Appendix VI*** *provides additional Sector Program sustainment tools.*



## Advice and Guidance for Implementing Effective Information Sharing

As a SC, look to be a *liaison* and *relationship manager* with those which you interact and participate closely within your industry. Share the knowledge of resources and availability of programs and connections with others. This will help ensure the broadest adoption and usage of systems and methods of information sharing, resilience and incident response.

Relationships are key to the success of gaining other’s trust and comfort with sharing their information. Memorandums of Understanding (MOU) and Non-Disclosure Agreements (NDA) may cover the formality of information sharing, but when the need is greatest, you want the sort of relationship where the partners and collaborators on the other end pick up the telephone and ask “How can I be of assistance?”

### Outreach

As a SC you should be leading the charge to bring the entities and individuals to the table for conversations to build trust and understanding. Know the [Sector-Specific Plan from DHS](https://www.dhs.gov/critical-infrastructure-sectors) and leverage the InfraGard Program as the reason for reaching out, this will help other parties see the purpose of your outreach.

Continue to advance partnerships by tracking action items from the discussion and driving future improvements; deliver what you promise as a way to build trust with those entities in which you will rely.

Don’t stop at the simple discussions; coordinate meetings with various sector owners and partners to understand how to support each other. Continually work to clarify the information that is valuable to all involved; you will find that many partners are willing to participate, but you will need to proactively engage them.

### Federal Agencies

#### Department of Homeland Security (DHS)

DHS clearly has been focused on CI and they have a multitude of resources and programs available in order to support and provide greater awareness and information sharing.

Start with your regional PSA or CSA this will allow you the opportunity to gain a deep understanding of programs and capabilities available to your IMA SSRP. Leverage DHS [Protected Critical Infrastructure Information Program[[6]](#footnote-7) (P](https://www.dhs.gov/pcii-program)CII) to protect information shared where applicable. Leverage the following resources or promote the programs / agencies where applicable.

##### [Automation Information Sharing (AIS)](file:///C:/Users/chuck/AppData/Local/Microsoft/Windows/INetCache/Content.Outlook/VZ8UOB4W/i.%09https:/www.dhs.gov/topic/cybersecurity-information-sharing) (May be available through Information Security Analysis Center (ISAC) services)[[7]](#footnote-8)

##### [Homeland Security Information Network (HSIN)](file:///C:/Users/chuck/AppData/Local/Microsoft/Windows/INetCache/Content.Outlook/VZ8UOB4W/i.%09https:/www.dhs.gov/homeland-security-information-network-hsin)

##### [Cyber Information Sharing and Collaboration Program (CISCP)](https://www.dhs.gov/ciscp)

##### [National Cybersecurity and Communications Integration Center (NCCIC)](https://www.dhs.gov/national-cybersecurity-and-communications-integration-center) (Serves as the hub of information sharing activities for the Nation to increase awareness of vulnerabilities, incidents, and mitigations.)

#### Federal Bureau of Investigation (FBI)

InfraGard is the FBI’s flagship partnership; however there are other opportunities and ways to get further involved and deepen partnerships. Reach out to your InfraGard coordinator about other partnerships and ways to deepen relationships; two example resources include:

##### CyWatch is the FBI’s 24-hour command center for cyber intrusion prevention and response operations.

##### [FBI Citizens Academy](https://www.fbi.gov/about/community-outreach).[[8]](#footnote-9)

##### Domestic Security Alliance Council (DSAC), a strategic partnership between the U.S. government and the U.S. private industry that enhances communication and promotes the timely and effective exchange of security and intelligence information between the federal government and the private sector.

#### United States Secret Service (USSS)

Depending on the sector and nature of the activity, you may have want to reach out to your relevant office of the Secret Service. Especially in metropolitan areas there is a local agent or office that you could reach out to in order to determine services that you may be able to promote or point members to. Many of the USSS offices have an Electronic Crimes Task Force that will have briefings for CI organizations.

#### Federal Emergency Management Agency (FEMA)

FEMA can be a great resource to leverage in planning exercises or getting involved in plan readiness activities. To locate your state and regional FEMA offices visit the [FEMA website](https://www.fema.gov/emergency-management-agencies).[[9]](#footnote-10) Your DHS PSA may also be able to coordinate with the local FEMA office.

### Sector Specific

Let’s face the facts, our industries have specific needs and face different threats; because of this Information Sharing and Analysis Organizations (ISAOs) and ISACs were created to cover this specialization. Below you will find resources to gain further information for your sector.

#### Information Sharing and Analysis Organizations (ISAOs) and Information Sharing and Analysis Centers (ISACs)

[ISACs](https://www.nationalisacs.org/member-isacs)[[10]](#footnote-11) – Make sure to promote and leverage your sector ISACs and make sure you understand the products and services they provide so you can promote the benefits of ISACs to your peers and InfraGard members.

[ISAOs](https://www.dhs.gov/isao)[[11]](#footnote-12) – Through public, open-ended engagements, ISAO will develop transparent best practices that align with the needs of all industry groups, not just those traditionally represented by ISACs

* ***Appendix VII*** *provides additional information on available ISAOs and ISACs.*



#### State and Local

Don’t overlook the value you can gain from State and Local resources. Partnering with these agencies or members from these areas of focus you may be able to access greater information sharing and resources than you can achieve via federal partners.

##### Emergency Management & Local Governments Cyber and Physical threats impact us all, no matter the protections and defenses we have will be impacted by greater events (attacks, weather, emergencies, etc.) which requires collaboration to respond during the crisis, and afterwards. By having conversations before the event you can ensure you have an understanding of the protocols and processes to leverage and interact during the moment of need. Include local police and fire in this discussion and how they plan response and recovery in order to support your CI sites and locations. You can find more references and information at the following site: [National Emergency Management Association (NEMA](https://www.nemaweb.org/index.php)) and Federal Emergency Management Agency (FEMA) Emergency Support Functions (ESF)[[12]](#footnote-13)

##### State Homeland Security Departments/Agencies

*Coordinate and support state efforts to prevent, protect against, and prepare for acts and threats of terrorism. They work with local, state and federal stakeholders to develop statewide strategic, operational and tactical plans for prevention and response, and offer or coordinate training and exercise opportunities to state, local, tribal, and private sector organizations.*

##### Fusion Centers Fusion Centers contribute to the Information Sharing Environment (ISE) through their role in receiving threat information from the federal government; analyzing that information in the context of their local environment; disseminating that information to local agencies; and gathering tips, leads, and suspicious activity reporting (SAR) from local agencies and the public. Most fusion centers will gladly vet and allow membership to mailing list and information sharing opportunities. Reach out to your nearest fusion center by looking [here](https://www.dhs.gov/fusion-center-locations-and-contact-information).[[13]](#footnote-14)

### Facilitating more effective Information sharing with the Traffic Light Protocol

The Traffic Light Protocol (TLP) was created by the international organization FIRST (Forum for Incident Response and Security Teams) to facilitate greater sharing of information. TLP has been adopted by both the National Institute for Standards and Technology (NIST) and United States Computer Emergency Response Team (US CERT).[[14]](#footnote-15)

TLP is a set of designations used to ensure that sensitive information is shared with the appropriate audience. It employs four colors to indicate expected sharing boundaries to be applied by the recipient(s). TLP provides a simple and intuitive schema for indicating when and how sensitive information can be shared, facilitating more frequent and effective collaboration.

TLP is not a “control marking” or classification scheme. TLP was not designed to handle licensing terms, handling and encryption rules, and restrictions on action or instrumentation of information. TLP labels and their definitions are not intended to have any effect on freedom of information or “sunshine” laws in any jurisdiction.

TLP is optimized for ease of adoption, human readability and person-to-person sharing. The source is responsible for ensuring that recipients of TLP information understand and can follow TLP sharing guidance. If a recipient needs to share the information more widely than indicated by the original TLP designation, they must obtain explicit permission from the original source.

* ***Useful Link*** *The following link provides additional information on the TLP standard for information sharing:* [*https://www.us-cert.gov/tlp*](https://www.us-cert.gov/tlp)*.*
* ***Appendix VIII*** *also provides additional TLP guidance.*



# Appendix I – Critical Infrastructure Sectors

This appendix provides detailed information for each DHS sector; you can see more information on the DHS website here: <https://www.dhs.gov/topic/critical-infrastructure-security>

|  |  |  |
| --- | --- | --- |
| SECTOR | DESIGNATED SECTOR-SPECIFIC AGENCY | NSSRP Trigraph |
| Chemical | Department of Homeland Security | CHM |
| Commercial Facilities | Department of Homeland Security | CMF |
| Communications | Department of Homeland Security | COM |
| Critical Manufacturing | Department of Homeland Security | CRM |
| Dams | Department of Homeland Security | DMS |
| Defense Industrial Base | Department of Defense | DIB |
| Emergency Services | Department of Homeland Security | ESS |
| Energy | Department of Energy | ENG |
| Financial Services | Department of Treasury | FIN |
| Food and Agriculture | Department of Agriculture and Department of Health and Human Services | FOD |
| Government Facilities | Department of Homeland Security and General Services Administration | GVF |
| Healthcare and Public Health | Department of Health and Human Services | HPH |
| Information Technology | Department of Homeland Security | INF |
| Nuclear Reactors/Materials/Waste | Department of Homeland Security | NUC |
| Transportation Systems | Department of Homeland Security and Department of Transportation | TRN |
| Water and Wastewater Systems | Environmental Protection Agency | WTR |

## Chemical

Composed of four main segments: Basic Chemicals; Special Chemicals; Life Sciences and Consumer Products. The sector is divided into five main segments, based on the product produced:

* Basic chemicals
* Specialty chemicals
* Agricultural chemicals
* Pharmaceuticals
* Consumer products

## Commercial Facilities

Largely private sector owned and operated Retail Establishments/Malls; Arenas. They operate on the standard of open public access to both ensure the general publics’ access to and freedom of movement throughout such facilities while minimizing the appearance of highly visible security barriers. The Commercial Facilities Sector consists of eight subsectors:

* Entertainment and Media (e.g., motion picture studios, broadcast media).
* Gaming (e.g., casinos).
* Lodging (e.g., hotels, motels, conference centers).
* Outdoor Events (e.g., theme and amusement parks, fairs, campgrounds, parades).
* Public Assembly (e.g., arenas, stadiums, aquariums, zoos, museums, convention centers).
* Real Estate (e.g., office and apartment buildings, condominiums, mixed use facilities, self-storage).
* Retail (e.g., retail centers and districts, shopping malls).
* Sports Leagues (e.g., professional sports leagues and federations).

## Communications

Industries that use terrestrial, satellite, and wireless transmission systems to provide communication abilities to the user.

## Critical Manufacturing

Consists of four broad manufacturing industries: primary metal manufacturing; machinery manufacturing; electrical equipment; appliance and component manufacturing; and transportation equipment manufacturing. Critical Manufacturing facilities include, but are not limited to, iron and steel mills, aluminum production, engine and transmission production, and motor vehicle, aerospace, and railroad rolling stock manufacturing. The Critical Manufacturing Sector identified the following industries to serve as the core of the sector:

* Primary Metal Manufacturing
  + - Iron and Steel Mills and Ferro Alloy Manufacturing
    - Alumina and Aluminum Production and Processing
    - Nonferrous Metal (except Aluminum) Production and Processing
    - Machinery Manufacturing
    - Engine, Turbine, and Power Transmission Equipment Manufacturing
* Electrical Equipment, Appliance, and Component Manufacturing
  + - Electrical Equipment Manufacturing
* Transportation Equipment Manufacturing
  + - Vehicle Manufacturing
    - Aviation and Aerospace Product and Parts Manufacturing
    - Railroad Rolling Stock Manufacturing

## Dams

Encompasses major infrastructure assets that harness the water resources of the nation and enable water management, balancing droughts and floods throughout the U.S.

## Defense Industrial Base

The Defense Industrial Base Sector is the worldwide industrial complex that enables research and development, as well as design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts, to meet U.S. military requirements.

The Defense Industrial Base partnership consists of Department of Defense components, more than 100,000 Defense Industrial Base companies and their subcontractors who perform under contract to the Department of Defense, companies providing incidental materials and services to the Department of Defense, and government-owned/contractor-operated and government-owned/government-operated facilities.

Defense Industrial Base companies include domestic and foreign entities, with production assets located in many countries. The sector provides products and services that are essential to mobilize, deploy, and sustain military operations.

The Defense Industrial Base Sector does not include the commercial infrastructure of providers of services such as power, communications, transportation, or utilities that the Department of Defense uses to meet military operational requirements. These commercial infrastructure assets are addressed by other Sector-Specific Agencies.

## Emergency Services

Representative of first-responder disciplines including: Emergency Management; Emergency Medical Services, Fire, Hazardous Material, Law Enforcement; Bomb Squads, Tactical Operations/Special Weapons & Assault Teams, and Search and Rescue organizations. Emergency Services functions, the majority of which are performed at the state, local, tribal, and territorial levels, are formally categorized by five disciplines:

* Law Enforcement
* Fire and Emergency Services
* Emergency Management
* Emergency Medical Services
* Public Works

This sector also provides specialized emergency services through individual personal teams. These specialized capabilities may be found in one or more various disciplines, depending on the jurisdiction:

* Tactical Teams (i.e. SWAT)
* Hazardous Devices Team/Public Safety Bomb Disposal
* Public Safety Dive Teams/Maritime Units
* Canine Units
* Aviation Units (i.e. police and medevac helicopters
* Hazardous Materials Teams
* Search and Rescue Teams
* Public Safety Answering Points (i.e. 9-1-1 call centers)
* Fusion Centers
* Private Security Guard Forces
* National Guard Civil Support

## Energy

Composed of the producers and providers of three interrelated segments:

* Electricity,
* Petroleum, and
* Natural Gas.

## Financial Services

Composed of banks, credit unions, and financial companies that allow users to deposit funds, make payments to other parties, invest funds for both long and short periods, provide credit and liquidity to customers, and transfer financial risks among customers.

## Food and Agriculture

Provides capacities to feed and clothe people well beyond America’s geographic boundaries. This sector accounts for roughly one-fifth of the Nation's economic activity and is overseen at the Federal level by the U.S. Departments of Agriculture and Health and Human Services and the Food and Drug Administration.

## Government Facilities

Includes a wide variety of buildings, owned or leased by federal, state, territorial, local or tribal governments, located domestically and overseas. This includes general-use office buildings and special-use military installations, embassies, courthouses, National laboratories, and structures that may house critical equipment and systems, networks and functions.

* **Education Facilities** Subsector covers pre-kindergarten through 12th grade schools, institutions of higher education, and business and trade schools. The subsector includes facilities owned by both government and private sector entities.
* **Elections Infrastructure** Subsector covers physical locations (storage facilities, polling places, and locations where votes are tabulated) and technology infrastructure (voter registration databases, voting systems, and other technology used to manage elections and to report and validate results). It does not include infrastructure related to political campaigns.
* **National Monuments and Icons Subsector** encompasses a diverse array of assets, networks, systems, and functions located throughout the United States. Many National Monuments and Icons assets are listed in either the National Register of Historic Places or the List of National Historic Landmarks.

## Information Technology

Comprised of, but not limited to, the following: Domain Name System (DNS) root and Generic Top-Level Domain Operators; Internet Service Providers (ISP); Internet Backbone Providers; Internet Portal and e-mail Providers; Networking Hardwired Companies; Networking Software Companies and Security Service Vendors.

## Nuclear Reactors, Materials and Waste

Includes nuclear power plants; non-power nuclear reactors used for research, testing and training; nuclear materials used in medical, industrial, and academic settings; nuclear fuel fabrication facilities, decommissioning reactors and the transportation, storage, and disposal of nuclear materials and waste.

## Healthcare and Public Health

Comprised of hospitals, clinics, and other care facilities dedicated to the maintenance and/or improvement of the health of their customers. The Public Health and Healthcare sector plays a significant role in response and recovery across all sectors in the event of a natural or manmade disaster.

## Transportation Systems

Consists of seven key subsectors or modes:

* **Aviation**: includes aircraft, air traffic control systems, and approximately 450 commercial airports and 19,000 additional airports, heliports, and landing strips. This mode includes civil and joint use military airports, heliports, short takeoff and landing ports, and seaplane bases.
* **Highway Infrastructure and Motor Carrier:** Encompasses nearly 4 million miles of roadway, almost 600,000 bridges, and some 400 tunnels in 35 states. Vehicles include automobiles, motorcycles, and trucks carrying hazardous materials, other commercial freight vehicles, motor coaches, and school buses.
* **Maritime Transportation Systems:** Consists of about 95,000 miles of coastline, 361 ports, 25,000 miles of waterways, 3.4 million square miles of Exclusive Economic Zone, and intermodal landside connections, which allow the various modes of transportation to move people and goods to, from, and on the water.
* **Mass Transit and Passenger Rail:** Includes service by buses, rail transit (commuter rail, heavy rail--also known as subways or metros--and light rail, including trolleys and streetcars), long- distance rail--namely Amtrak and Alaska Railroad--and other, less common types of service (cable cars, inclined planes, funiculars, and automated guideway systems).
* **Pipeline Systems:** Consists of vast networks of pipeline that traverse hundreds of thousands of miles throughout the country, carrying nearly all of the nation's natural gas and about 65 percent of hazardous liquids, as well as various chemicals. These include approximately 2.2 million miles of natural gas distribution pipelines, about 168,900 miles of hazardous liquid pipelines, and more than 109 liquefied natural gas processing and storage facilities.
* **Freight Rail:** Consists of seven major carriers, hundreds of smaller railroads, over 140,000 miles of active railroad, over 1.3 million freight cars, and roughly 20,000 locomotives. Further, over 12,000 trains operate daily. The Department of Defense has designated 30,000 miles of track and structure as critical to mobilization and resupply of U.S. forces.
* **Postal and Shipping:** Moves over 574 million messages, products, and financial transactions each day. Postal and shipping activity is differentiated from general cargo operations by its focus on letter or flat mail, publications, or small- and medium- size packages and by service from millions of senders to nearly 152 million destinations.

## Water and Wastewater Systems

Capacities providing the means to deliver potable and non-potable water products and services. There are approximately 153,000 public drinking water systems and more than 16,000 publicly owned wastewater treatment systems in the United States. More than 80 percent of the U.S. population receives their potable water from these drinking water systems, and about 75 percent of the U.S. population has its sanitary sewerage treated by these wastewater systems.

# Appendix II – RENS Implementation Support

This appendix provides detailed questions for each of the four activities that a successful IMA SSRP would engage in: Recruitment; Education; Networking; and Information Sharing. Use these questions to effect how you:

* Develop annual SSRP planning;
* Shape the activities you engage in to build and sustain your IMA SSRP;
* Communicate to others what the SSRP is seeking to achieve;
* Evaluate how well your IMA is performing; and
* Identify areas for improvement within your IMA SSRP.

**RENS Questions**

**1. Recruitment**

* Do you have representation from all of the significant (sector specific) organizations/agencies involved in owning or operating CI in your chapters area?
* Do you have a list of other organizations/agencies within your sector who should be members of your chapter?
* What are you doing to recruit members of your sector into the chapter?
* What challenges are you facing with recruiting members into your SC program?
* Do you need some help with recruiting sector members?

**2. Education**

* Have you asked members of your sector what educational areas/subjects they would like to see?
* Do you have access to threat/risk assessment reports (for your sector) that you can use to develop an education program for members of your sector?
* Have you assembled a list of potential speakers on subjects related to your sector?
* Do you interact with other SCs/local SIGs to use them to offer training to members of your sector?
* Do you need some help developing education opportunities for members of your sector?

**3. Networking**

1. Do members of your sector get a chance to network/talk to each other about the threats/risks they face?
2. Do you have a formal program to setup events where members of your sector can talk/network with each other? (separate from education)
3. Have you engaged other associations (related to your sector) that can offer networking opportunities for members of your sector?
4. Have you **worked** with other local SCs to offer networking opportunities between related sectors in your chapter? (like health and IT)
5. Do you interact with other IMA chapter SCs (for your sector) in development of your program? (new)
6. Do you need some help developing networking opportunities for members of your sector?

**4. Information Sharing**

1. What mechanisms are available in your chapter for two-way information sharing with the FBI, DHS, fusion center, etc?
2. Do you have a good relationship with these agencies, one that includes good two-way information sharing?
3. How is the relationship between your sector members and the FBI? (also DHS, Local Fusion Center, etc?)
4. Are there things that you (or your chapter) do to promote better information sharing?
5. Do you need some help developing better two-way information sharing?

# Appendix III – National Sector Chief Selection Process

NSCs will be selected through a competitive process, led by the NSSRP Program Manager. When directed by the InfraGard National Board, or when there is a vacancy on the NSCC, the NSSRP Program Manager will invoke the following process to select new NSCs:

1. The NSSRP Program Manager will prepare a NSCC Solicitation and present it to the InfraGard National Chairman for approval-for-release. This solicitation will identify the sectors from which candidates are being sought and specific selection criteria candidates will need to meet.
2. When approved, the InfraGard National Executive Director will disseminate the solicitation to all InfraGard National members.
3. Candidates desiring consideration for NSCC position shall prepare and submit an abbreviated resume (not to exceed two pages) highlighting their experiences that qualify them for the position.
4. Candidates must also submit a statement (not to exceed one page) to describe:
   1. Why they want to hold the position; and
   2. What they see as the strategic objectives or opportunities they would work towards in the position.
5. The NSSRP Program Manager will provide an online survey tool that candidates will use to apply and submit required documentation, no later than the date noted in the solicitation.
6. The NSSRP Program Manager will solicit at least two other members of the NSCC to evaluate the received submissions.
7. The NSSRP Program Manager will summarize the findings of the review panel and prepare a report of recommendation for candidates to be appointed to the available NSCC positions.
8. The NSSRP Program Manager will also contact the home IMA President for each selected candidate to ensure there are no issues with their selection to the NSCC.
9. Once the candidate vetting is complete, the NSSRP Program Manager will forward a report of recommendations to the InfraGard National Chairman for ratification by the InfraGard National Board.
10. The InfraGard National Chairman will share the findings to the InfraGard National Board for ratification of the NSSRP Program Manager recommendations.
11. Once appointed the NSSRP Program Manager will prepare and deliver appointment letter(s) to the selected NSCs; a copy of the appointment letter(s) will be forward to the InfraGard National Executive Director.
12. The ratified NSC will serve a complete two calendar-year term commencing January 1 following the date of appointment.

# Appendix IV – IMA Sector Chief Selection, Employment, and Evaluation Tools

This appendix *provides an example* process for selecting IMA SCs, a template job description for those selected as a SC, and an evaluation tool to assess IMA SC engagement and effectiveness. IMAs should tailor this to fit local needs.

**IMA Sector Chief Job Description**

Provided below is a *sample job description* for an IMA SC; each IMA should tailor this job description to fit their specific SSRP scope and needs.

**INFRAGARD [ENTER IMA NAME] SECTOR CHIEF JOB DESCRIPTION**

**TITLE**: Sector Chief

**REPORTS TO**: IMA President or Designee

**JOB PURPOSE**: To enhance timely, accurate and effective dissemination of sector specific information to protect the nation’s CI by providing comprehensive expertise in each sector to assist all FBI Field Offices and IMAs in protecting CI in their areas of responsibility.

### **JOB DUTIES:**

1. Obtain and demonstrate knowledge of priority threats of FBI Field Office annually or as required by turnover.
2. Regularly distribute sector specific information to/from FBI PSCs and sector members.
3. Encourage your sector members to provide information to the FBI via FBI PSCs and/or iGuardian.
4. Serve as spokesperson/POC for the sector.
5. Communicate regularly ( at least quarterly by email, webinar, telephone and/or in person with your sector members for two way sharing of information and collaboration, continuing education, resolution of issues, determination of needs, etc.)
6. Communicate with other SCs in your IMA President at least quarterly for two-way cross-sector information sharing and collaboration as needed or requested.
7. Communicate with your NSC (when appointed) as needed for two-way sharing of information and the best ways to motivate and educate sector members.
8. Assist your IMA with member recruitment and retention as necessary or requested.
9. Seek opportunities and/or initiate trainings, exercises, continuing education meetings at least quarterly.
10. Initiate and participate in projects and initiative at regional and national levels as necessary or requested.
11. Perform other related duties as needed or requested.

### **QUALIFICATIONS:**

1. Motivated leader within the IMA membership and/or member of professional organizations related to the sector.
2. Subject matter expert and/or important stakeholder who has a good understanding and knowledge of the sector with interest in CI protection.
3. Strong communication skills.
4. Access to networking opportunities and the ability to build effective relationships within the infrastructures and communities, such as local intelligence/Fusion Centers, DHS PSA, CSA, and other public or regulatory agencies.
5. Agrees to and signs a Non Disclosure Agreement.
6. Understands he/she may be placed in a position to receive and disseminate classified information with the proper security clearance.

### **TERMS OF OFFICE**

It is recommended the SC is appointed for one year terms by IMA President and FBI PSC, and ratified by the IMA Board.

**IMA Sector Chief Evaluation Tool**

Provided below is a sample IMA SC evaluation tool; each IMA should tailor this tool to fit their specific SSRP scope and needs.

**IMA SECTOR CHIEF EVALUATION CRITERIA**

IMA SECTOR CHIEF JOB DUTIES EVALUATION CRITERIA *SATISFACTORY NEEDS WORK*

1. Obtain and demonstrate knowledge of priority threats of FBI Field Office once a year or as required by turnover.

COMMENTS

1. Regularly distribute sector specific information to/from FBI PSCs and sector members.

COMMENTS

1. Encourages sector members to provide tips to the FBI via FBI PSCs and/or iGuardian.

COMMENTS

1. Serve as spokesperson/POC for the sector.

COMMENTS

1. Communicates regularly (at least quarterly by email, webinar, telephone and/or in-person) with sector members for two-way sharing of information and collaboration, continuing education, resolution of issues, determination of needs, etc.

COMMENTS

1. Communicates with other SCs in your IMA your IMA President at least quarterly for two-way cross-sector information sharing and collaboration as needed or requested.

COMMENTS

1. Communicates with NSC (as appointed) as needed for two-way sharing of information and the best ways to motivate and educate sector members.

COMMENTS

1. Assists IMA with member recruitment and retention as necessary or requested.

COMMENTS

1. Seeks opportunities and/or initiate trainings, exercises, continuing education meetings at least quarterly.

COMMENTS

1. Initiates and participates in projects and initiatives at regional and national levels as necessary or as requested.

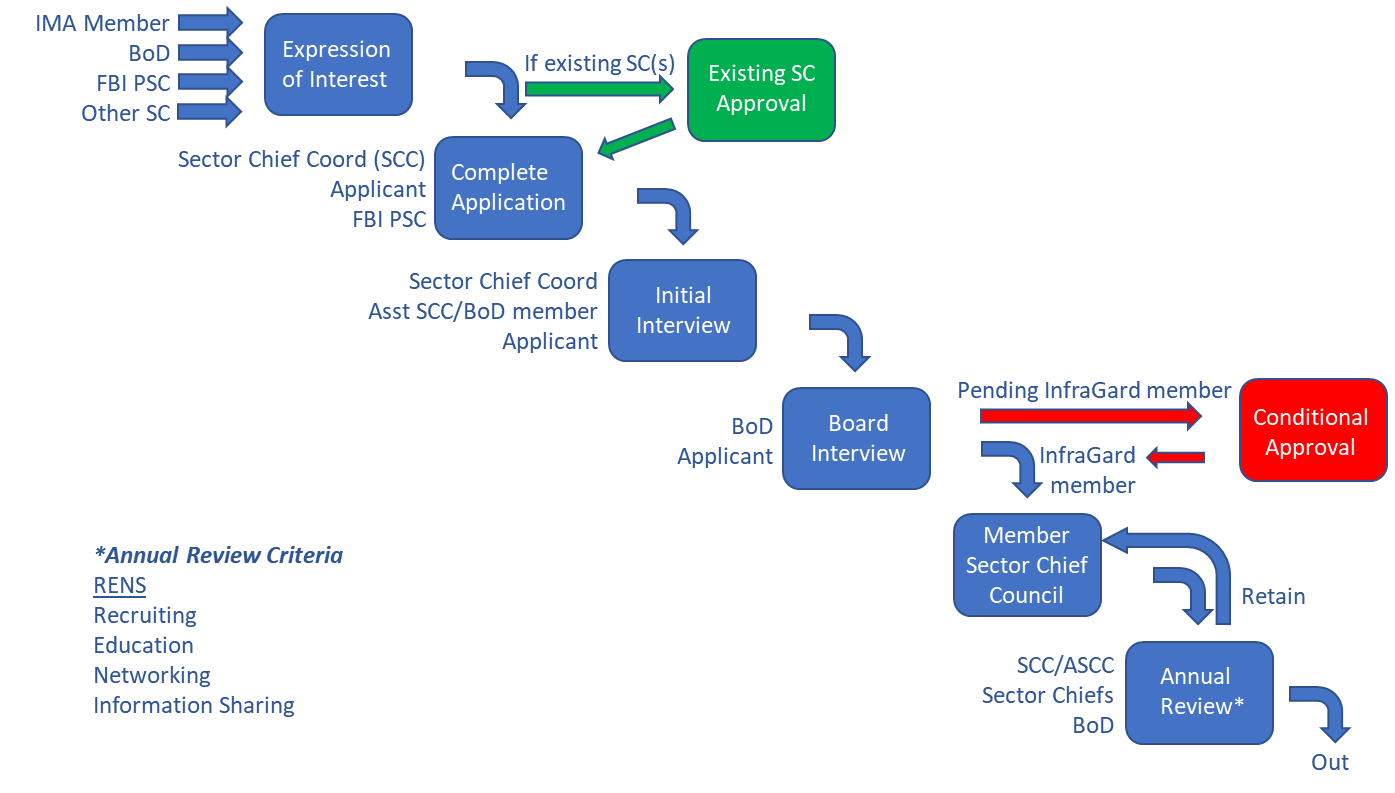
COMMENTS

**RECOMMENDATIONS FOR IMPROVEMENT**

# Appendix V – IMA San Diego (Example) Sector Chief Selection/Lifecycle Process

Each IMA should develop a process for selecting qualified SCs. As an example, below is presented the process that the San Diego IMA uses; each IMA should tailor the process to fit their specific SSRP scope and needs.

## San Diego Sector Chief Selection/Lifecycle Process Flow Diagram



## San Diego Sector Chief Selection Process Description

As with any other personnel recruiting and hiring process, the chances of landing an active and effective InfraGard Sector Chief improves markedly when they are formally recruited, vetted and approved by the IMA Board of Directors.

In many cases, IMAs are so relieved to find a Sector Chief volunteer that they just assign a title and hope for the best. Figure 1 above provides a roadmap to a much sounder alternative that allows Sector Chief candidates an opportunity to state their vision and understanding of what the role entails.

Sector Chiefs can be nominated from several sources as shown but as a minimum must be active InfraGard members. If multiple (or Deputy) Sector Chiefs are used, the existing team should be consulted regarding the desirability of adding a new member.

An initial interview tests the applicant for his/her commitment to the role, their understanding of the requirements and if they have a vision going forward to support the IMA. A formal scheduled interview with the Board of Directors would follow the informal interview and if an active InfraGard member, the candidate can be approved by the Board.

At this point it is imperative that the Board update its IMA records with InfraGard National and the FBI to validate and record the change. If the candidate’s InfraGard membership is still under review, the approval process can be conditional as shown in the figure.

Once a Sector Chief joins an IMA’s Sector Chief Council, annual reviews will ensure that all Sector Chiefs are performing at least minimal activities during the year. The review process should focus on the RENS criteria described earlier in this Handbook: Recruiting, Education, Networking and Information Sharing.

This process or a similar alternative, will allow the IMA to select the most motivated and capable Sector Chief candidates and help ensure a viable Sector Chief program.

# Appendix VI – IMA SSRP Sustainment Tools

## Critical Infrastructure Protection “7 Factors for the Future” –

Presentation for IT Sector; double click the diagram below to open the presentation (Word version only):



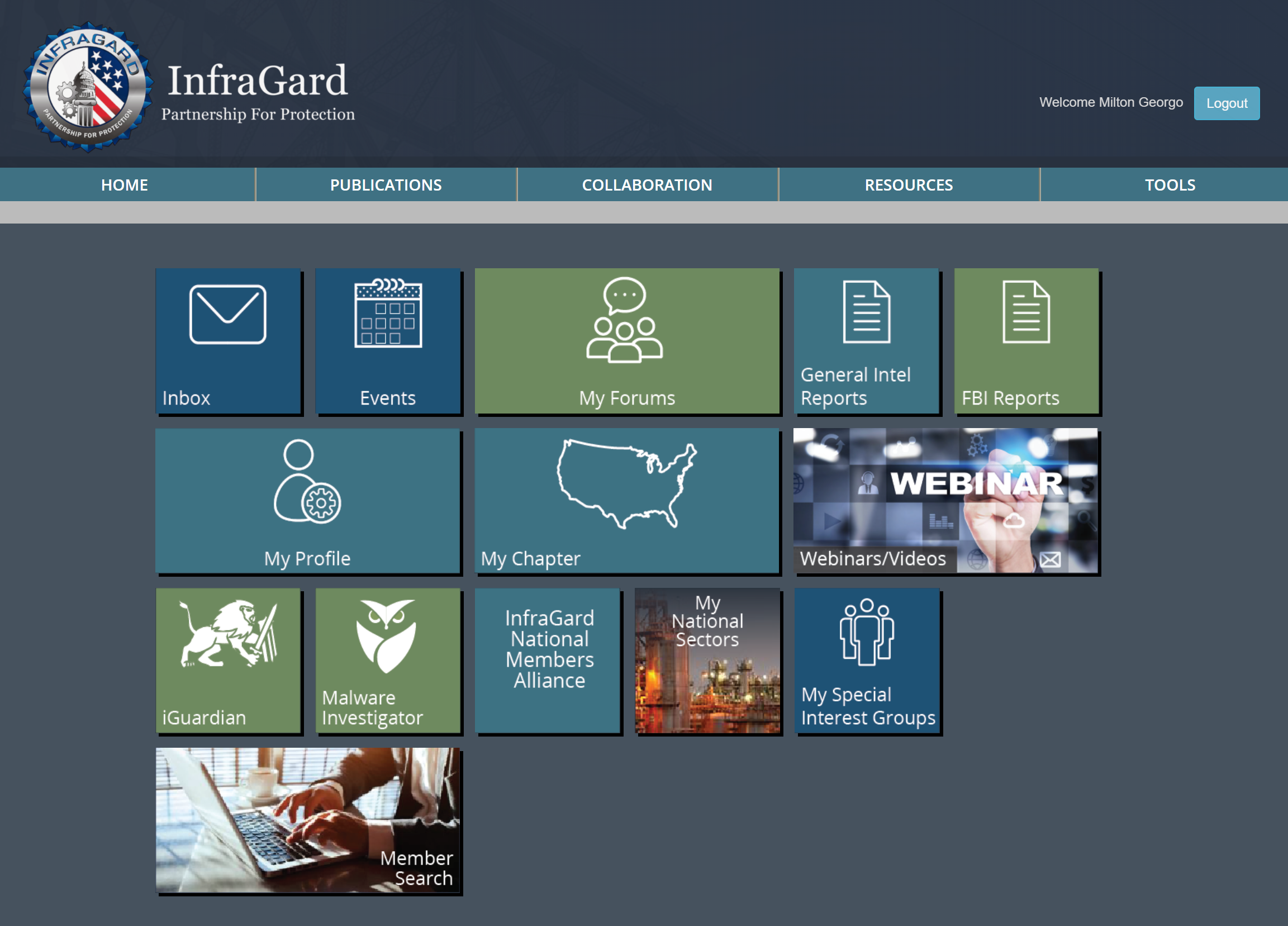
## FBI Secure Portal

InfraGard members have access to an FBI secure communications portal featuring an encrypted website, web mail, forums, and message boards. The website plays an integral part of InfraGard National and NSSRP information-sharing efforts; we use it to:

* Disseminate threat alerts and advisories;
* Send out intelligence products from the Bureau and other agencies;
* Enable members to securely communicate with one another;
* Access a number of tools and other websites in support of the CI Protection (CIP) mission; and
* Provides discussion forums for secure collaboration on topics related to CIP.

The portal also now includes NSSRP-specific forums for NSCs, SMEs, and InfraGard members to discuss threats, vulnerabilities, and other matters pertaining to an individual sector.

Below is a screen capture of the InfraGard portal “dashboard” that provides easy access to all capabilities and content.



## Homeland Security Information Network-Critical Infrastructure (HSIN-CI)

Successful CI Protection (CIP) requires coordination and collaboration between CI owners and operators, the DHS, other Federal agencies, and State and Local government.

This strategic and operational CIP coordination and collaboration happens within the CI Information Sharing Environment (CI ISE). The CI ISE’s primary collaboration tool is HSIN-CI.

HSIN-CI is a secure, unclassified, web-based communications system that serves as the primary, nationwide DHS collaboration system for sharing Sensitive But Unclassified (SBU) information. HSIN-CI supports the CI ISE by serving as a common platform to provide tactical and planning communication functionality for private sector CI owners and operators. To access HSIN visit: <https://hsin.dhs.gov/Pages/home.aspx>

DHS has designated HSIN-CI to be its primary information sharing platform between and within the CI sectors and State and Local Fusion Centers. HSIN-CI enables DHS and the CI sector stakeholders to communicate, coordinate and share information in support of the Sector Partnership Framework at no charge to sector stakeholders.

It goes without saying that this element of HSIN-CI relies upon an existing and functional relationship between the local IMA and its DHS fusion center. In turn a strong Sector Chief program at the IMA level will greatly facilitate this partnership.

Through HSIN-CI, users can:

* Receive, submit and discuss timely, actionable and accurate information
* Maintain a direct, trusted channel with DHS and other vetted sector stakeholders
* Communicate information pertaining to threats, vulnerabilities, security, response and recovery activities affecting sector and cross sector operations

All SCs should have, or apply for HSIN-CI access; visit this website for more information: <https://www.dhs.gov/how-join-hsin>.

Below is a screen capture of the HSIN-CI Portal.



## Zoom Meetings

IMAs, their SSRP Coordinator, and their SCs can request from InfraGard National use of the Zoom Webinar platform. Local SSRPs can use the Zoom platform to hold meetings and to conduct webinars; visit <https://zoom.us/> for more information about the platform. To schedule use of the Zoom platform, email the InfraGard National Executive Director at [executivedirector@infragardmembers.org](mailto:executivedirector@infragardmembers.org).

# Appendix VII – ISACs/ISAOs

|  |  |  |
| --- | --- | --- |
| ISAC | SECTOR | SPONSOR/OPERATOR |
| AutoISAC | Transportation | Auto-ISAC Board of Directors |
| Aviation ISAC\* (A-ISAC) | Transportation | Airports Council International |
| Chemical ISAC\*\* (ChemISAC) | Chemical | American Chemistry Council |
| Communications ISAC\* | Telecommunications | National Coordinating Center for Communications |
| Defense Industrial Base ISAC\* (DIB-ISAC) | Defense Industrial Base | DIB ISAC |
| Downstream Natural Gas ISAC\* (DNG-ISAC) | Energy | American Gas Association |
| Elections Infrastructure ISAC  (EI-ISAC) | Government Facilities | Center for Internet Security |
| Emergency Management & Response ISAC\* (EMR-ISAC) | Emergency Services | U.S. Fire Administration (FEMA) |
| Electricity Sector ISAC\* (E-ISAC) | Energy | North American Energy Reliability Corporation |
| Financial Services ISAC\* (FS-ISAC) | Banking & Finance | NC4™ |
| Food ISAC | Food & Agriculture | Food Marketing Institute |
| IT ISAC\* | Information Technology | IT ISAC |
| Maritime ISAC\* | Transportation | Maritime Security Council |
| Multi-State ISAC\* (MS-ISAC) | IT (Cyber Security) | Center for Internet Security |
| National Defense ISAC | Defense Industrial Base | National Defense ISAC |
| National Health ISAC\* (NH-ISAC) | Healthcare & Public Health | Global Situational Awareness Center (NASA/Kennedy Space Center (Host); NH-ISAC West, San Diego CA |
| Oil & Natural Gas ISAC\* (ONG-ISAC) | Energy, IT | National Petroleum Council |
| Over The Road Bus ISAC\* (ORTB-ISAC) | Transportation | EWA-IIT (host) |
| Public Transportation ISAC\*  (PT-ISAC) | Transportation | American Public Transportation Association |
| Real Estate ISAC\* (RE-ISAC) | Commercial Services | Real Estate Roundtable |
| Higher Education & Research ISAC\* (REN-ISAC) | Government Facilities, IT | Indiana University (Host Facility) |
| Supply Chain ISAC\* | Transportation, IT | International Cargo Security Council |
| Surface Transportation ISAC\* (ST-ISAC) | Transportation | Association of American Railroads; EWA-Information & Infrastructure Technology (Host Facility) |
| Water ISAC\* | Water & Wastewater | Association of Metropolitan Water Agencies |

ISACs in red have a primary Cyber focus  
\* member of the National Council of ISACs  
\*\* currently inactive

# Appendix VIII – Traffic Light Program Detailed Guidance

This appendix provides detailed information about each level of the TLP.

|  |  |  |
| --- | --- | --- |
| Color | When should it be used? | How may it be shared? |
| TLP:RED   Not for disclosure, restricted to participants only. | Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused. | Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person. |
| TLP:AMBER   Limited disclosure, restricted to participants’ organizations. | Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. | Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.** |
| TLP:GREEN   Limited disclosure, restricted to the community. | Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. | Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community. |
| TLP:WHITE   Disclosure is not limited. | Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. | Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. |

1. Each NSC and their respective SMEs, together, for a *national sector council* for that respective sector. For example, the NSC and SMEs for the Communications sector would form the “National Communications Sector Council (NCSC), the NSC and SMEs for the Information Technology sector would form the National Information Technology Sector Council (NITSC), and so on for the other NSCs. [↑](#footnote-ref-2)
2. See Appendix I for a list of all sixteen sectors [↑](#footnote-ref-3)
3. Note: To encourage broad engagement in the NSSRP, the NSC selection process only allows one NSC to come from the same company or government agency. [↑](#footnote-ref-4)
4. Appendix III provides a description of the National Sector Chief Selection Process [↑](#footnote-ref-5)
5. Note: To encourage broad engagement in the NSSRP by IMAs, the SME selection process only allows one SME per sector to come from the same IMA, company, or government agency. [↑](#footnote-ref-6)
6. <https://www.dhs.gov/pcii-program> [↑](#footnote-ref-7)
7. <https://www.nationalisacs.org/about-isacs> [↑](#footnote-ref-8)
8. <https://www.fbi.gov/about/community-outreach> [↑](#footnote-ref-9)
9. <https://www.fema.gov/emergency-management-agencies> [↑](#footnote-ref-10)
10. <https://www.nationalisacs.org/member-isacs> [↑](#footnote-ref-11)
11. <https://www.dhs.gov/isao> [↑](#footnote-ref-12)
12. NEMA information: <https://www.nemaweb.org/index.php> and ESF information: <https://emilms.fema.gov/is230c/fem0104160text.htm> [↑](#footnote-ref-13)
13. Fusion center locations: <https://www.dhs.gov/fusion-center-locations-and-contact-information> [↑](#footnote-ref-14)
14. NIST TLP information: <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-150.pdf> and US CERT TLP information: <https://www.us-cert.gov/tlp> [↑](#footnote-ref-15)