Critical Infrastructure Threat Information Sharing Framework

A Reference Guide for the Critical Infrastructure Community

October 2016

Homeland Security

Page intentionally left blank.

Contents

Quick Reference Guide for Critical Infrastructure Owners and Operators[1, 2]

Report Threats and Incidents

- In an emergency, call 9-1-1, report suspicious activity and threats to federal facilities at 1-877-4FPS-411 (1-877-437-7411)
- Contact your local law enforcement agency
- Report through your organization's appropriate internal reporting process
- Directly report non-emergency threats and incidents to your nearest FBI field office at https://www.fbi.gov/contact-us/field or nearest international office at https://www.fbi.gov/contact-us/legat
  - Report threats and crime online at https://www.fbi.gov/report-threats-and-crime
  - Report suspicious activity involving chemical, biological, or radiological materials, by calling (toll-free) 1-855-TELL-FBI (1-855-835-5324)
  - Report an online scam or email hoax by filing a complaint online with the Internet Crime Complaint Center at http://www.ic3.gov/complaint/default.aspx or by using the online Tips and Public Leads form at https://tips.fbi.gov/
  - Provide information on select major cases by calling the Major Case Contact Center at 1-800-CALL-FBI (1-800-225-5324)

Report Suspicious Activity

To report suspicious activity, contact your local law enforcement agency. Describe specifically what you observed, including:

- **Who** or **what** you saw, including the suspicious username and a screenshot if online
- **When** you saw it
- **Where** it occurred, including web link if online
- **Why** it's suspicious
- **How** the incident took place (i.e., how did the suspect enter the building, how did you discover something was abnormal)

If there is an emergency, call 9-1-1.

WHY REPORT INCIDENTS?

Cybercrimes and incidents require data to solve. When incidents get reported with the best available data, law enforcement and security professionals have a better chance of solving crimes and preventing future impacts from not only the actors involved, but also those that are using the same infrastructure or tools.

[1] This Framework focuses on information sharing based on the *National Infrastructure Protection Plan (NIPP) 2013* structures; however, some sectors, such as the Chemical, Nuclear, Healthcare, and Public Health Sectors, have regulatory requirements to report incidents to their regulatory program. This Framework does not address those regulatory requirements.

[2] As described in Section 1.2 Purpose and Scope, this Framework's scope is limited to manmade threats.

Report Suspected or Known Cyber Incidents

- Contact the National Cybersecurity and Communications Integration Center (NCCIC) at https://www.dhs.gov/about-national-cybersecurity-communications-integration-center, nccic@hq.dhs.gov, or 1-888-282-0870
- For more information, see the NCCIC's entity description on page 31
- Contact the nearest FBI Field Office: http://www.fbi.gov/contact-us/field
- See a two-page summary on Cyber Incident Reporting, including when, what, and how to report cyber incidents to the Federal Government (directed towards law enforcement, but also relevant to critical infrastructure owners and operators): https://dhs.gov/sites/default/files/publications/Law Enforcement Cyber Incident Reporting.pdf

Report Physical Infrastructure Incidents

- Email the National Infrastructure Coordinating Center (NICC) at NICC@hq.dhs.gov or call (202) 282-9201
- Contact your sector's Information Sharing and Analysis Organization (ISAO) or Information Sharing and Analysis Center (ISAC), and/or Sector-Specific Agency (SSA)

Become a Partner in the "If You See Something, Say Something™" Campaign

- Visit https://www.dhs.gov/see-something-say-something/become-partner for more information

Receive Threat Information Relevant to Your Sector

There are a variety of ways to receive threat information. Critical infrastructure owners and operators will likely want to connect with more than one of the entities listed below to establish an ongoing information-sharing relationship. The ones best suited for your organization may depend on your needs, capabilities, and interests. See the entity descriptions in Section 3 starting on page 21 for more detailed information about these and other threat information-sharing entities.

- Contact your local law enforcement agency (see Local and State Law Enforcement Operations Centers entity description on page 30 for more information)
- Contact your nearest FBI Field Office https://www.fbi.gov/contact-us/field (see FBI Field Offices entity description on page 23 for more information)
- Join the Homeland Security Information Network – Critical Infrastructure (HSIN-CI) https://www.dhs.gov/hsin-ci (see NICC entity description on page 33 for more information)
- Join a Regional Consortium Coordinating Council (RC3) member organization in your area —Membership application and links to Council members: http://RC3US.org
- Join InfraGard—Membership application and access to InfraGard's Secure Web Portal: http://www.infragard.org. Join your sector's or region's ISAO or your sector's ISAC

- See the ISAO entity description on page 27 and the ISAC entity description on page 26 for more information, including a full list of ISACs' websites, or visit the National Council of ISACs website: http://www.isaccouncil.org

- Contact your nearest State or major urban area fusion center and ask for a briefing, or establish an information-sharing relationship
  - Find your nearest fusion center: http://www.dhs.gov/contact-fusion-centers
  - Connect with the fusion center's liaison officer for private sector outreach
  - See the fusion center entity description on page 25 for more information
  - Contact your SSA or Sector Coordinating Council (SCC)See page 38 for a description of SCCs and a list of Sector Coordinating Councils and their websites
  - For charters and information on the sectors for Sector Coordinating Councils and Government Coordinating Councils, see https://www.dhs.gov/critical-infrastructure-partnership-advisory-council
  - See page 40 for a description of SSAs and page 41 for a list of SSAs and their contact information

Access Threat Prevention and Protection Related Training and Exercises

- See https://www.dhs.gov/critical-infrastructure-training for a wide array of free training designed to improve the knowledge and skills needed to implement critical infrastructure security and resilience activities, including active shooter and improvised explosive device preparedness
- Free online Suspicious Activity Reporting (SAR) training for the private sector and other hometown security partners is available at https://nsi.ncirc.gov/training_online.aspx
- Contact your nearest FBI field office, which has outreach coordinators in each of its 56 field offices. See page 23 for a full list of training and educational information
  - For more information about the FBI's Community Outreach, visit https://www.fbi.gov/about-us/partnerships_and_outreach/community_outreach and https://www.fbi.gov/about/partnerships/office-of-partner-engagement/active-shooter-incidents
- Contact your nearest fusion center (page 25), nearest Department of Homeland Security (DHS) Office of Infrastructure Protection's (IP) Protective Security Advisor (PSA) (page 37), sector's ISAC (page 26), or Sector Coordinating Council (SCC) (page 38) for more opportunities

Page intentionally left blank.

Executive Summary

This Framework is a resource to help critical infrastructure owners and operators, as well as other private sector, Federal, and State, local, tribal, and territorial (SLTT) government partners that share threat information, learn where they can turn, and in what circumstances, to both receive and report threat information. Threat information in this Framework is limited to information sharing pertaining to manmade threats, including both cyber and physical threats, to critical infrastructure.

This document is not new policy, but describes the various processes and mechanisms currently used to share threat information and the existing array of threat information-sharing entities involved in those processes. It was developed in response to a need for greater clarity identified by the critical infrastructure community, and supports the 2012 *National Strategy for Information Sharing and Safeguarding* (NSISS)[3] as well as the *National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience* (NIPP 2013)[4] Call to Action to build upon partnership efforts and one of its goals to share actionable and relevant information across the critical infrastructure community.

Section 1 provides the background, purpose, scope, and intended audience for the Framework. It also identifies information-sharing guiding principles selected from the most pertinent strategy and policy documents relevant to this Framework. Section 2 provides an overview of the threat information-sharing process and types of threat information-sharing entities by category. Section 3 provides a collection of one-page descriptions of the major threat information-sharing partners involved in the threat information-sharing process described in the previous section. The descriptions include contact information, products and services available for owners and operators, and situations during which to contact that particular entity.

Section 4 offers four use cases to illustrate how threat information sharing actually happened in real world situations and they provide insight into the kinds of exchanges that happen in the critical infrastructure community. The use cases are:

1. Cyber: Havex and BlackEnergy (2014)
2. Physical: Metcalf Electric Substation Attack (2013)
3. International: Westgate Mall Attack in Kenya (2013)
4. National Special Security Event: 2013 Presidential Inauguration

Using the NIPP council structure, this Framework was developed by a working group composed of private sector, Federal, and SLTT representatives across the infrastructure community. The effort was co-led by the Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS). Participants across various sectors of the critical infrastructure community evaluated current threats, the current information-sharing environment, needed areas for improvement, and specific requirements related to threat information sharing. Feedback was solicited and incorporated throughout the development process.

---

[3] The White House, *National Strategy for Information Sharing and Safeguarding* (NSISS), December 2012 , https://www.whitehouse.gov/sites/default/files/docs/2012sharingstrategy_1.pdf (accessed June 17, 2016).

[4] U.S. Department of Homeland Security, *National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience*, https://www.dhs.gov/sites/default/files/publications/National-Infrastructure-Protection-Plan-2013-508.pdf (accessed June 17, 2016). The NIPP 2013 is the successor to the National Infrastructure Protection Plan 2010.

Page intentionally left blank.

SECTION 1

Introduction

Our national security depends on the nation's ability to share the right information, with the right people, at the right time.[5]

— 2012 National Strategy for Information Sharing and Safeguarding (NSISS)

1.1 Background

The Nation's critical infrastructure[6] provides the essential services that underpin American society and serve as the backbone of our nation's economy, security, and health. We know it as the power we use in our homes, the water we drink, the transportation that moves us, the stores we shop in, and the communication systems we rely on to stay in touch with friends and family. The risk environment surrounding critical infrastructure is complex and uncertain as threats, vulnerabilities, and consequences continue to evolve. For example, critical infrastructure that has long been subject to risks associated with physical threats and natural disasters is now increasingly subject to cyber risks. Growing interdependencies across critical infrastructure systems have increased the type and scope of potential consequences resulting from the compromise of underlying systems or networks.[7] Given the importance of critical infrastructure to the functioning of our Nation, it is vital to keep these systems and assets secure and resilient in the face of evolving and increasingly complex hazards and threats.

As described in the *National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience* (NIPP 2013) (the successor to the *National Infrastructure Protection Plan 2010*),[8] issued pursuant to *Presidential Policy Directive 21 (PPD-21), Critical Infrastructure Security and Resilience*,[9] much of the critical infrastructure in the United States is owned and/or operated by the private sector.[10] Thus, in order to ensure the security and resilience of the Nation's critical infrastructure, the Federal Government must develop a robust partnership with critical infrastructure owners and operators. Strengthening and maintaining secure and resilient critical infrastructure does not solely depend on adequate investment and physical and virtual protection of our critical assets and systems. Coordinated efforts and partnerships between the private and public sectors also depend on effective and efficient information sharing among critical infrastructure owners and operators, the Federal

---

5 The White House, *National Strategy for Information Sharing and Safeguarding* (NSISS), December 2012, https://www.whitehouse.gov/sites/default/files/docs/2012sharingstrategy_1.pdf (accessed June 17, 2016), 1.

6 As defined in the U.S. Patriot Act (H.R. 3162, 107th Congress, 2001), critical infrastructure is the "systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

7 U.S. Department of Homeland Security, *National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience*, https://www.dhs.gov/sites/default/files/publications/National-Infrastructure-Protection-Plan-2013-508.pdf (accessed June 17, 2016), 8.

8 More information on the NIPP 2013 can be found at https://www.dhs.gov/national-infrastructure-protection-plan (accessed June 17, 2016).

9 PPD-21 can be found at https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (accessed June 17, 2016).

10 Federal, State, and local government entities also own and operate critical infrastructure.

Government, and the critical infrastructure community[11] at large. Recognizing this, one of the five goals articulated in the NIPP 2013 focuses on critical infrastructure information sharing:

> Share actionable and relevant information across the critical infrastructure community to build awareness and enable risk-informed decision making.[12]

Critical infrastructure information sharing better prepares all stakeholders to assess critical infrastructure vulnerabilities, address those vulnerabilities, understand potential incident consequences, and prevent, protect against, mitigate, respond to, and recover from threats and attacks. Efforts to improve Federal Government information sharing with State and local governments, the private sector and, in particular, the critical infrastructure community, continue to evolve to address new threats, vulnerabilities, and technologies, while respecting privacy, civil liberties, and the need for reasonable information safeguards.

1.2 Purpose and Scope

The purpose of this Framework is to describe the current processes used to facilitate the flow of threat information between and among all entities involved in the critical infrastructure security and resilience mission, and provide an overview of the key threat information-sharing entities which facilitate this process. The intention is to help critical infrastructure owners and operators and other entities better understand where and how to participate in receiving and sharing threat information with information-sharing hubs.

Since the attacks of September 11, 2001, the U.S. Government has worked to improve standardized information sharing across multiple disciplines and communities. Though this Framework focuses on the critical infrastructure community, it recognizes the information-sharing processes are multidisciplinary in nature. This Framework does not present new policy and relies on existing authorities, strategies, policies, plans, and practices that define the roles and responsibilities of Federal departments and agencies, as well as the other entities in the critical infrastructure community, which share threat information.[13]

This Framework's scope is limited to threat information sharing pertaining to manmade threats, including both cyber and physical threats, to critical infrastructure.[14] Some sectors, such as the Chemical, Nuclear, Healthcare, and Public Health Sectors, have regulatory requirements for owners and operators to report incidents to their regulators. This Framework does not address those requirements.

The vision of this Framework is to strengthen the effective and efficient sharing of accurate, actionable, timely, and relevant threat information between and among the Federal

---

[11] Defined in the NIPP 2013, the critical infrastructure community includes critical infrastructure owners and operators, both public and private; trade associations; Federal departments and agencies; regional entities; SLTT governments; and other organizations from the private and nonprofit sectors with a role in securing and strengthening the resilience of the Nation's critical infrastructure and/or promoting ideas for doing so, and in some cases, foreign government partners.

[12] NIPP 2013, 5.

[13] Due to the primary audience of this document (critical infrastructure owners and operators (see Section 1.3)), it is outside the scope of this document to identify all such authorities and policies. Such information is captured in the 2007 *National Strategy for Information Sharing* and other policy documents which can be found at www.ise.gov.

[14] This Framework is not a summary of the 2012 NSISS, NIPP 2013, or the various mission frameworks per PPD-8 or the Information Sharing Environment. There are a variety of information-sharing practices, processes, and programs throughout government. This Framework is meant to focus exclusively on the critical infrastructure threat piece. Likewise, response related information and information flows are covered under PPD-8 related documents and the Response Framework.

Government, critical infrastructure owners and operators, and other entities. Such sharing builds situational awareness, enables effective risk-informed decision-making,[15] and therefore increases the security and resilience of U.S. critical infrastructure.

1.3 Audience

The primary audience for this Framework is the critical infrastructure community, with an emphasis on critical infrastructure owners and operators—including privately and publicly owned critical infrastructure—and relevant private sector information-sharing entities, including Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs).

In addition to serving the primary audience, this Framework is intended to serve as a useful point of reference for the wide-ranging critical infrastructure community, including Sector-Specific Agencies (SSAs);[16] Federal centers, such as the National Infrastructure Coordinating Center (NICC) and the National Cybersecurity and Communications Integration Center (NCCIC);[17] State, local, tribal, and territorial (SLTT) governments; and other entities involved in the threat information-sharing process. For example, since physical critical infrastructure is located within and, therefore, subject to specific SLTT jurisdictions, SLTT government entities have important responsibilities to prevent, protect against, mitigate the consequences of, respond to, and recover from the host of threats and hazards that can impact critical infrastructure. SLTT government entities, such as State and major urban area fusion centers (fusion centers),[18] also provide important geographical context, analytic capabilities, and subject-matter expertise for their jurisdictions, enhancing the flow of threat information between the Federal Government and the private sector.

1.4 Guiding Principles

This Framework adheres to the guiding principles outlined in the 2012 *National Strategy for Information Sharing and Safeguarding* (NSISS),[19] the core tenets of the NIPP 2013, and the guidance for the Information Sharing Environment.[20] Recognizing that the 16 critical

---

15 NIPP 2013.

16 PPD-21 defines a "Sector-Specific Agency" (SSA) as the Federal department or agency designated under this directive to be responsible for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment.

17 The national critical infrastructure centers as described in PPD-21.

18 For more information on fusion centers, see the entity description in Section 3 page 25.

19 The 2012 NSISS is the President's plan for how the Federal Government will responsibly share and safeguard information that enhances national security and protects the safety of the American people. It can be found at https://www.whitehouse.gov/sites/default/files/docs/2012sharingstrategy_1.pdf (accessed June 17, 2016).

20 The Information Sharing Environment (ISE) is defined as the people (Federal, State, regional, local government, and private sector entities), projects, systems, and agencies that enable responsible information sharing across the national security enterprise. The ISE was established by the Intelligence Reform and Terrorism Prevention Act of 2004—a direct result of 9/11 Commission recommendations. The ISE is administratively run by the Program Manager for the Information Sharing Environment (PM-ISE) who has government-wide authority to plan, oversee, and manage the ISE. Appointed by the President, the PM-ISE also co-chairs of the White House Information Sharing and Access Interagency Policy Committee (ISA-IPC). The role of the PM-ISE is to coordinate and facilitate the development of a network-centric information sharing environment for terrorism and homeland security information by focusing on standards and architecture, security and access, associated privacy protections, and best practices. PM-ISE serves as a change agent and center for innovation and discovery in providing ideas, tools, and resources to mission partners who then apply them to their own agencies or communities.

infrastructure sectors[21] are diverse in their composition, threats, vulnerabilities, assets, systems, and regulatory regimes, this Framework supports a wide range of sector perspectives, operations, and levels of decision-making.

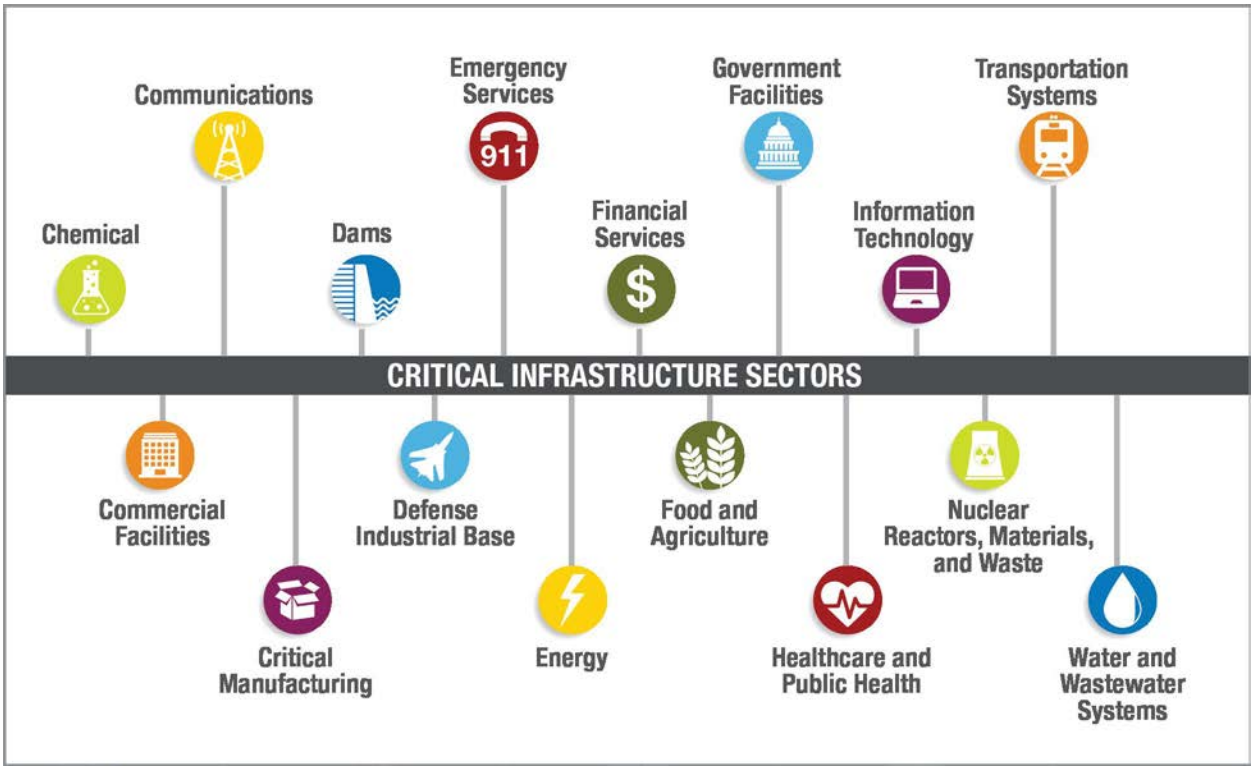


Figure 1: The 16 Critical Infrastructure Sectors

The following principles of threat information sharing were identified from the NSISS during development of this Framework. These principles should be considered when sharing threat information.

1. **To inform effective decision-making, information being shared should be accurate, relevant, timely, and actionable.**

2. **To be most effective, information sharing must be multidirectional. Threat information, when applicable, should be shared with critical infrastructure partners at the appropriate classification level, and as much as possible at the unclassified level.** Providing access to specific and actionable unclassified threat information, such as "tearlines,"[22] JIBs, briefings, etc., will enable the greatest number of stakeholders to share within their organizations and take actions to mitigate threats.

3. **The risks associated with information sharing and safeguarding are reduced through the adoption of sound policies and standards.** Building trust in sharing and

[21] PPD-21 defines the 16 critical infrastructure sectors.

[22] Tearline information is defined as intelligence information that has been sanitized (by removal of sources and methods) so it may be disseminated at a lower classification. Source: Joint Counterterrorism Assessment Team (JCAT) Intelligence Guide for First Responders, https://www.ise.gov/sites/default/files/Intelligence%20Guide%20for%20First%20Responders_web.pdf (accessed June 17, 2016).

> safeguarding requires the ability to manage risk. Risk to national security increases when the approach to information sharing is inconsistent, fragmented, or managed from a single-agency perspective. Risk decreases with sound policies and standards, increased awareness and comprehensive training, effective governance, and enhanced accountability.[23]

In addition, the development of this Framework was informed by the National Institute of Standards and Technology's draft *Guide to Cyber Threat Information Sharing* (NIST Special Publication 800-150).[24]

1.5 Development Methodology

Using the NIPP council structure, this Framework was developed by a working group composed of private sector, Federal, and SLTT representatives across the infrastructure community. The effort was co-led by the Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS). Participants across various sectors of the critical infrastructure community evaluated current threats, the current information sharing environment, needed areas for improvement, and specific requirements related to threat information sharing. Feedback was solicited and incorporated throughout the development process.

[23] NSISS, 7.

[24] The second draft of NIST's Special Publication 800-150 was released April 2016 and has not been released in final form at the time of writing. It can be found at http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-150 (accessed June 17, 2016).

Page intentionally left blank.

SECTION 2

Overview of Critical Infrastructure Security and Resilience Threat Information Sharing

This Framework articulates a flexible, adaptive, and networked approach to sharing threat information that relies primarily, but not exclusively, on designated information-sharing hubs[25] that have roles and responsibilities in the critical infrastructure security and resilience mission and that leverage standards, baseline capabilities, and/or standard operating procedures (SOPs) to ensure information flows to and from all critical infrastructure partners. This Framework also reflects the need for flexibility and scalability and allows for the importance and utility of informal networks,[26] enabling ad hoc point-to-point communications when necessary. A flexible framework enables effective response to evolving threats while abiding by various safeguards and restrictions on sharing. A scalable framework enables the scope of information sharing to expand and contract given the specific threat.

As noted in Section 1, this Framework does not present new policy. This approach is built on the principles identified in the U.S. Government's national security strategies and plans which recognize that our country's size, free market, and system of federalism, combined with the evolving and multi-faceted nature of the threats confronting the U.S., demands that the U.S. leverage a "Whole-of-Government" and "Whole-Community" approach to preventing and mitigating threats. The Federal Government partners with and relies on SLTT governments, the private sector, and citizens to prevent, protect against, respond to, mitigate, and recover from a variety of threats. This approach relies heavily on effective information sharing with all partners.

This Framework documents the current and evolving environment and identifies the key hubs and other participants within the network through which information flows. It emphasizes those entities with a direct connection to critical infrastructure owners and operators (i.e., those entities with whom owners and operators can either share or receive information). This Framework also recognizes that there are many entities throughout the law enforcement, homeland security, and intelligence communities that produce information that may be valuable to critical infrastructure owners and operators, even if those entities do not have direct interaction with owners and operators.

A critical part of this Framework and the information-sharing process described herein is the idea that information-sharing hubs are best positioned to assess information within the context of their expertise and the community they serve. Examples of information-sharing hubs within the Federal Government include the FBI Terrorist Screening Center (TSC), the National Counterterrorism Center (NCTC), the National Infrastructure Coordinating Center (NICC), and

[25] Information-sharing hubs (hubs) are described more fully in Section 2.1. Generally, hubs are entities that aggregate, integrate, validate, assess, and analyze information, and produce and share products. This Framework focuses on hubs that produce threat information that is relevant to the critical infrastructure security and resilience mission.

[26] There is no official definition of informal information-sharing networks. Generally, they rely upon personal contacts and are ad hoc in nature. Individuals sometimes use informal networks to circumvent perceived or real process or organization barriers or challenges. The use of the term in this Framework is to acknowledge that authorized sharing does occur outside of the information sharing hubs and the process described in Section 2.1 and that such sharing is embraced as a healthy part of the threat information sharing ecosystem provided that such sharing is done in a manner that complies with all information safeguarding requirements and protects privacy and civil liberties.

the National Cybersecurity and Communications Integration Center (NCCIC).[27] Though each of these entities has distinct missions and roles, they are all part of the information-sharing process. The following examples of nonfederal information-sharing hubs also demonstrate their importance in the information-sharing ecosystem:

- **Fusion Centers:**[28] The 2007 National Strategy for Information Sharing (NSIS) recognized and codified the roles and responsibilities for State and major urban area fusion centers in the Information Sharing Environment. Specifically, it called for the establishment of a national integrated network of fusion centers, and designated fusion centers as the "focus, but not exclusive points, within the State and local environment for the receipt and sharing of terrorism information, homeland security information, and law enforcement information related to terrorism."[29] Fusion centers are owned and operated by State and local agencies. Some fusion centers were established prior to the attacks of September 11, 2001, but the concept gained momentum thereafter, and, by 2005, existing fusion centers had collaboratively developed fusion center guidelines. Later, they established baseline capabilities for fusion centers. The Federal Government supports fusion centers through a variety of resources, including classified and unclassified systems access, personnel, and grant funding.
- **Information Sharing and Analysis Centers (ISACs):**[30] ISACs were established and are managed by consortiums of critical infrastructure owners and operators to provide comprehensive critical infrastructure sector analysis within the sector, other sectors, and with government. They are largely made up of private sector entities. Though capabilities vary, the Federal Government makes efforts to establish operational relationships with ISACs.

CYBER INFORMATION SHARING

As a discipline, cybersecurity is a rapidly evolving field, and new government and private sector organizations are being established to address all its evolving facets. The relatively nascent nature of the field reflects an environment in which frequent updates to laws, regulations, policies, and guidance are needed, which subsequently leads to changes in the procedures and protocols for the sharing of cyber threat information. The high-level information-sharing process described in this Framework was drafted to cover the main actions that take place regardless of whether the threat is cyber or physical. Despite the fact that there will likely be changes in cyber threat information-sharing organizations, rules, and protocols in the near future, the working group believes the general principles and processes described in the Framework will remain valid for the years to come. The reader is encouraged to visit the resources provided in the entity descriptions (Section 3) to review more detailed information about cyber information sharing mechanisms and processes.

[27] For a more detailed categorization of information sharing hubs, see Section 2.2. For descriptions of these and other entities, please see Section 3.

[28] This description is intended to show how fusion centers are an example of an information sharing hub. For more information on fusion centers, see the more comprehensive description in Section 3 page 25.

[29] The 2012 NSSIS explicitly affirmed the 2007 NSIS.

[30] This description is intended to show how ISACs are an example of an information sharing hub. For more information on ISACs, see the more comprehensive description on page 26.

- **Information Sharing and Analysis Organizations (ISAOs):**[31] The Federal Government is encouraging the development of voluntary standards and guidelines for the creation and functioning of ISAOs that share information across a region, sector, subsector, or in response to a specific emerging cyber threat. The ISAO Standards Organization (ISAO-SO), led by the University of Texas at San Antonio, was established October 1, 2015, and is working with the critical infrastructure community to identify a common set of voluntary standards for the creation and functioning of ISAOs as required by Executive Order 13691, *Promoting Private Sector Cybersecurity Information Sharing*.[32]

The Federal Government's support of information-sharing hubs that adhere to common standards and capabilities ensures information flows efficiently and effectively while also allowing for independence among entities and mission diversity.

2.1 Threat Information-Sharing Process

This section provides an overview of the critical infrastructure threat information-sharing process and the types of entities that participate in the critical infrastructure threat information-sharing process.

Once it is received, information flows between and among government entities and the private sector through a multidirectional, flexible, decentralized "network" characterized by both formal and informal channels, which are described in the entity descriptions and variety of case studies provided in Sections 3 and 4, respectively. However, despite its diversity, the networked information flows can be summarized in the steps below. How certain steps are carried out is often dictated by an organization's internal rules, requirements, and procedures. This process overview is not intended to imply that organizations should change their procedures, nor should individuals ignore their internal requirements.

[31] This description is intended to show how ISAOs are an example of an information sharing hub. For more information on ISAOs, see the more comprehensive description on page 27.

[32] Executive Order 13691 can be found at https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari (accessed June 20, 2016).

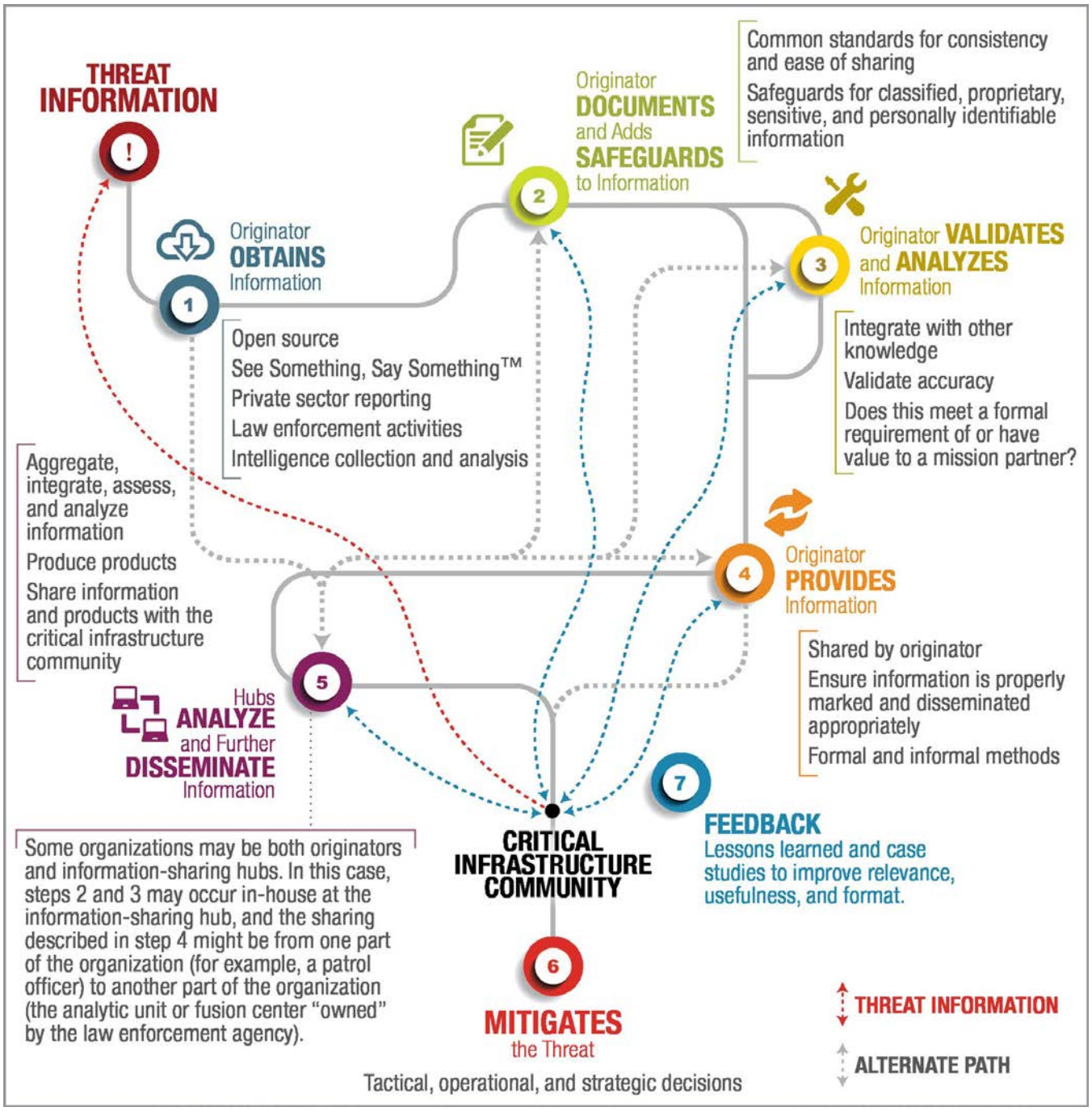


Figure 2: Threat Information-Sharing Process

This graphic is not fully representative of the multidirectional, decentralized network of formal and informal channels through which government entities and the private sector share information. It is intended only to show the basic steps of the information flow. Depending on the size of the originating entity, certain steps may occur informally and simultaneously. Details of each step are described in the narrative below.

Step 1: Originator Obtains Information[33]

Information is obtained from a variety of sources (e.g., open source, confidential, law enforcement, intelligence, public, and private) and methods (e.g., investigations, assessments, and intelligence collection). For example, a private company's public safety or security personnel observe a security vulnerability trend at their facility or on their IT networks; local, State, or Federal law enforcement glean information from law enforcement activities (e.g., investigations, routine enforcement, etc.); a citizen notices suspicious activity; or the Federal Government's Intelligence Community (IC)[34] identifies a credible threat.

Step 2: Originator Documents and Adds Safeguards to Information

A best practice is for organizations to develop and publish threat and incident reporting processes, including how and when information should be sent to other organizations, such as information-sharing hubs. As appropriate, entities should follow their internal agency reporting procedures.

Typically, each entity has processes for documenting information obtained through legal means and for an authorized purpose.

- Common standards have been developed to assist Federal and SLTT law enforcement in documenting information consistently. Standardization allows for information to be shared more easily. For example, the Suspicious Activities Reporting (SAR)[35] process defines data elements and a common process to be used for facilitating the assessment and sharing of such information in an appropriate manner.

In the documentation process, information is "marked" to indicate the required level of safeguards and any restrictions on authorized access or use. For example:

- If obtained by the IC, the information may be marked at the required classification level.
- If obtained through law enforcement sources, it may be marked Law Enforcement Sensitive (LES).
- If the information contains personally identifiable information (PII), markings should comply with entity, local, State, and Federal regulations and guidelines. Organizations often require authorized recipients to have received related training and agree to abide by the rules prior to receiving the information.[36]

---

[33] At the beginning of the process, it is not necessarily clear whether or not information is a threat.

[34] The Intelligence Community (IC) is a group of Executive Branch agencies and organizations that work separately and collaboratively to engage in intelligence activities that are necessary for the conduct of foreign relations and the protection of the national security of the United States. These activities include collection of information needed by the President, the National Security Council, the Secretaries of State and Defense, and other Executive Branch officials for the performance of their duties and fulfillment of their responsibilities. They produce and disseminate intelligence and protect against hostile activities directed against the United States. The IC is led by the Director of National Intelligence (DNI), who is the head of the Office of the Director of National Intelligence (ODNI) and whose duty is to coordinate the other 16 IC components based on intelligence consumers' needs. *U.S. National Intelligence: An Overview 2013*. For more information, contact Partner.Engagement@dni.gov.

[35] For more information about the Nationwide Suspicious Activity Reporting Initiative (NSI), go to https://nsi.ncirc.gov/default.aspx (accessed June 21, 2016).

[36] The IC's protocols are by far the strictest, requiring recipients to hold clearances (which in and of itself requires extensive steps associated with obtaining and maintaining clearances), sign legally binding agreements to protect information, and receive annual training on the handling classified information.

- Many ISACs and other organizations use the Traffic Light Protocol (TLP),[37] [38] a set of designations used to ensure that sensitive information is shared with the correct audience. It employs four colors to indicate different degrees of sensitivity and the corresponding sharing considerations to be applied by the recipient(s).

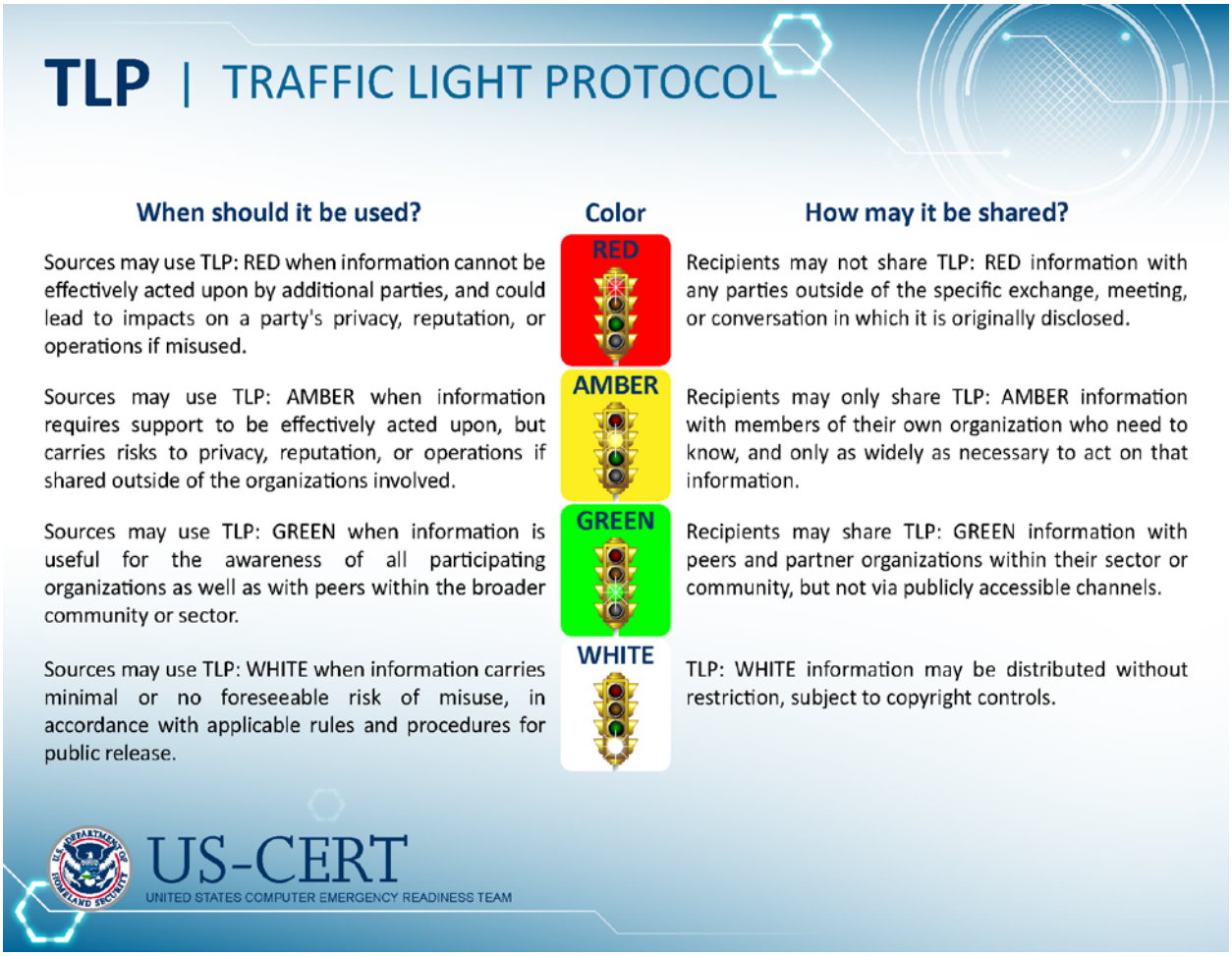


Figure 3: Traffic Light Protocol

Step 3: Originator Validates and Analyzes Information

Originators, to the extent they are able, integrate the information with other knowledge and validate the information's accuracy. The originator should consider whether the information meets a formal information requirement of a partner or may have value to the larger critical infrastructure community. For a very small entity, this step may occur informally and simultaneously with Steps 1 and 2 above.

[37] See https://www.us-cert.gov/tlp for more information. In addition to US-CERT and other domestic communities of cybersecurity practitioners, TLP is also employed by public and private sector organizations within Australia, Canada, Finland, France, Germany, Hungary, Italy, Japan, Netherlands, New Zealand, Norway, Sweden, Switzerland, and the United Kingdom.

[38] TLP does not apply to classified information. The Controlled Unclassified Information (CUI) program seeks to standardize the way U.S. Executive departments and agencies handle sensitive but unclassified (SBU) information, including information marked as "For Official Use Only (FOUO)," "Law Enforcement Sensitive (LES)," and others. It should be noted that the TLP designations are not a category or subcategory under the CUI program.

Step 4: Originator Provides the Information Pursuant to Access and Use Restrictions

Consistent with decisions made in Step 2 for safeguarding, the originator determines who has a need to know the information generated in compliance with relevant laws and regulations. Many organizations, including the Federal Government's IC, law enforcement, ISACs, and ISAOs establish standard protocols for marking and handling information. The originator may provide information through informal networks (i.e., word of mouth, emails to colleagues, phone calls, or routine meetings), as well as formal channels, including when the originator shares information with a hub[39] for discrete or larger distribution.

- Format:
  - The format and content of the information shared depends on the originator and the nature of the information.
  - If the IC[40] has information that may eventually be shared with the private sector, products are sent to the FBI and DHS with appropriate tearlines at multiple classification levels, to include unclassified if possible, so that FBI and/or DHS can develop products targeted to specific audiences.
  - Information derived from the private sector or local or State law enforcement may be "sanitized," consistent with step 2.
  - Formal analytic products are typically not produced before sending to hubs. The exceptions may be if the originator is a Sector-Specific Agency (SSA), a very large metropolitan law enforcement organization, or a very large company with analytic cadres.
- Mechanisms for Sharing:
  - Typically, information is sent to the information-sharing hubs through secured, electronic mechanisms such as the Homeland Security Information Network – Critical Infrastructure (HSIN-CI) managed by DHS.[41]
  - Sharing may also occur through in-person briefings or joint conference calls. For example, the DHS Office of Infrastructure Protection (IP) and the Partnership for Critical Infrastructure Security Cross Sector Council(s) developed a document, *Coordination Plan for Targeted Threat and Security Engagement*, describing a process by which IP and the CSCs share information.[42] The plan defines procedures for conducting targeted engagements focused on intelligence and security information regarding physical and cyber threats.
  - Classified information must be shared through channels and mechanisms approved for classified information sharing.

---

[39] See Section 3, Threat Information Sharing Entity Descriptions, for descriptions of various information-sharing hubs, which include government operation centers, State and major urban area fusion centers, ISACs and ISAOs with formal watch centers, and law enforcement entities, such as the FBI's DSAC and InfraGard etc.

[40] For further information about how the Federal Government's Intelligence Community receives, analyzes, and shares intelligence information, please see the *Joint Counterterrorism Assessment Team Intelligence Guide for First Responders*: https://www.ise.gov/sites/default/files/Intelligence%20Guide%20for%20First%20Responders_web.pdf (accessed June 21, 2016).

[41] For a list of information sharing mechanisms, see Appendix E.

[42] For additional information about the Coordination Plan for Targeted Threat and Security Engagements, see Appendix F.

- Automated machine-to-machine exchanges are becoming increasingly common to speed up threat information sharing, especially related to cyber threats. Many such systems[43] use Trusted Automated eXchange of Indicator Information (TAXII) as the preferred method of exchanging information using the Structured Threat Information eXpression (STIX) language, to create an automated, machine-readable feed of threat and security information that can be shared across industries and groups in near-real time.[44] See entity descriptions in Section 3 for details on methods of sharing.

Step 5: Hubs Aggregate, Integrate, Validate, Assess, and Analyze Information; Produce and Share Products

Hubs, by design, are aware of the information requirements of their various partners or customers. Thus they are well positioned to assess whether information requires additional analysis and whether it should be shared with other partners.

- Once in receipt of information, hubs will perform their own validation and analysis—integrating the new information with other knowledge and determining whether it should be passed along to other partners, and if so, how to tailor for their use.
- If a determination is made to provide information to other partners, the hub may conduct additional analysis and produce an official product. (Product types can vary based on the hub and customer or stakeholder requirements.)
- Safeguards may be reassessed in light of the integration, analysis, and target audience for the product.
- Information is provided to the hub's partners, which may include other hubs, through a variety of mechanisms (e.g., secure web portals which allow for posting of information or intelligence bulletins, direct one-on-one phone calls, conference calls, briefings, etc.).

Step 6: Mitigating the Threat

The critical infrastructure community receives the information and makes tactical, operational, and strategic decisions to help mitigate the threat. The types of actions taken depend on the roles and responsibilities of the entity. For example, owners and operators may make tactical decisions to strengthen their protective measures, while associations or program and policy entities may develop new training to be deployed across the country.

Step 7: Feedback Loop

An important component of the information-sharing cycle is the feedback recipients of the information provide to the originators and producers of analytic products to improve relevance, usefulness, and format.

---

[43] Examples of machine-to-machine information exchanges include the Enhanced Cybersecurity Services (ECS) offered by DHS; the Security Event System and its Collective Intelligence Framework component, from the Research and Education Networking Information Sharing and Analysis Center (REN-ISAC); and Public Regional Information Security Event Management (PRISEM) from the State of Washington.

[44] For more information, see http://measurablesecurity.mitre.org/docs/stix-intro-handout.pdf and https://www.oasis-open.org/news/pr/oasis-advances-automated-cyber-threat-intelligence-sharing-with-stix-taxii-cybox (accessed June 21, 2016).

Regardless of whether the sharing is vertical (to/from the Federal Government and SLTT entities and owners and operators) or horizontal (e.g., owners and operators to owners and operators/state to state, etc.), common steps are taken to determine what is shared, with whom, when, and how. In particular, the role of the information-sharing hubs, such as the Federal Government's operation centers, InfraGard, fusion centers, and ISACs, are critical to efficient and effective information sharing with the private sector. (Please see the entity descriptions in Section 3 for a list and description of the various information-sharing hubs.) These hubs also allow for and recognize that informal networks and personal relationships are a necessary and important part of effectively sharing threat information with the private sector.

Utilizing information-sharing hubs enables the integration of critical infrastructure owners and operators and private sector security partners, as appropriate, into the threat information-sharing ecosystem. Moreover, with standards in place for use, access restrictions, and information security, sector partners are reassured that the integrity and confidentiality of their sensitive information can and will be protected and that the information-sharing process can produce actionable information regarding threats.

2.2 Types of Entities Participating in the Threat Information-Sharing Process

The broad threat information-sharing ecosystem and the similar roles and responsibilities different entities share can be delineated into categories to align with the roles they play in the information-sharing process. Some of the entities referenced fall under more than one category. The categorization of threat information-sharing entities that follows does not represent new policy nor does it override existing relationships.

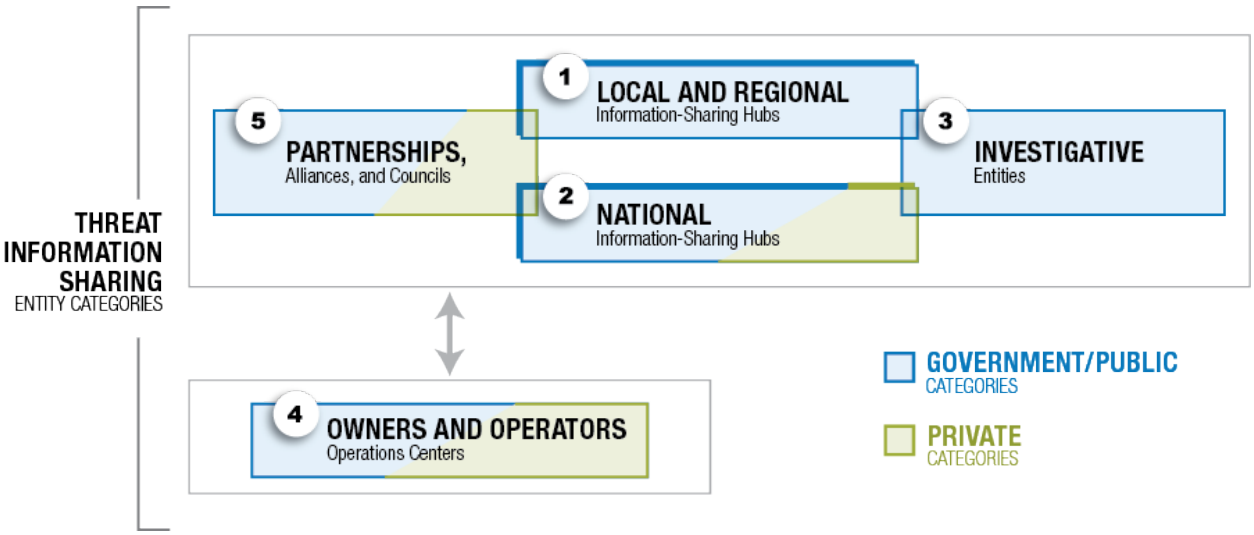


Figure 4: Categories of Threat Information-Sharing Entities

Category one and two (illustrated in Figure 4) are information-sharing hubs that aggregate the threat information received and then provide that information to their partners. They participate in and often facilitate both vertical and horizontal information flows. They are often operations centers, analysis centers, or watch centers. Many operate on a 24x7 basis. The other three

categories, “Investigative,” “Owners and Operators,” and “Partnerships,” are included to show how they interact with information-sharing hubs and the information-sharing process.

The rest of this section provides examples of entities in each category, and Section 3 includes further descriptions of select entities deemed by the working group to be most relevant to owners and operators regarding threat information sharing.

ONLINE PLATFORMS

This Framework and the categories in this section focus on entities sharing threat information. Online information-sharing platforms, such as HSIN, also play an important role in the threat information-sharing process, and are included in the description of the entity that manages them (i.e., information on HSIN-CI is included in the NICC entity description). For a non-exhaustive list of relevant threat information-sharing platforms, see Appendix E: Threat Information-Sharing Mechanisms and Sources, and Tools to Assess Threats.

2.2.1 Local and Regional Information Sharing Hubs

Local and regional information-sharing hubs operate locally or regionally primarily serving a local or regional customer set. They have relationships with national hubs and often serve as the conduit between owners and operators and Federal Government agencies’ headquarters offices. These entities represent both State and local governments and the Federal Government.

Figure 5: Local and Regional Information-Sharing Hubs

2.2.2 National Information Sharing Hubs

National information-sharing hubs are operations, analysis, and/or watch centers responsible for a national perspective. In some cases, the products they create are shared through local or regionally based information-sharing hubs. Many of these entities have a much broader mission than critical infrastructure security and resilience.[45]

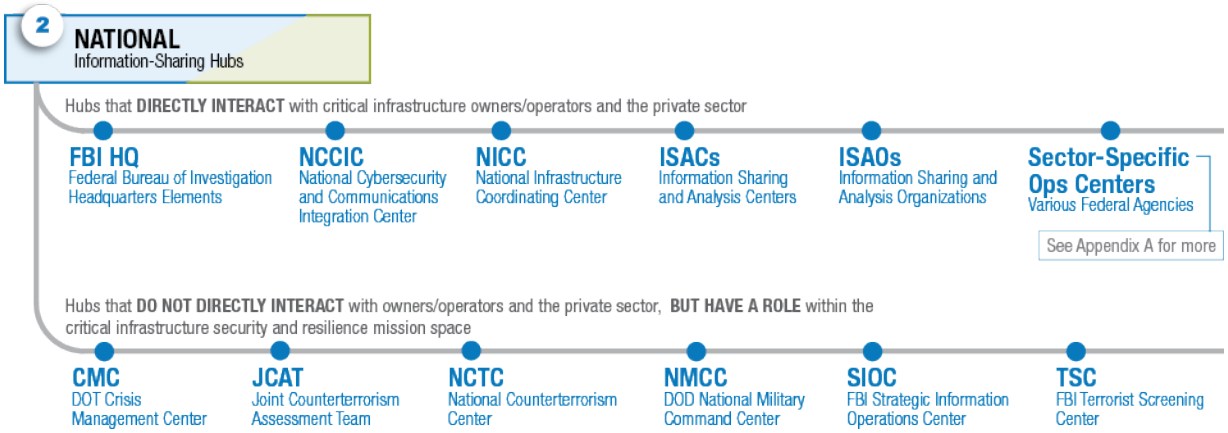


Figure 6: National Information-Sharing Hubs

2.2.3 Investigative Entities

Investigative entities are not primarily "public facing." Their primary purpose is to conduct law enforcement investigations. Typically, investigative entities do not routinely work or share information with owners and operators unless they are providing threat briefings or investigating a specific matter relevant to the owner or operator. However, they may receive tips or suspicious activity reports from an owner or operator of critical infrastructure. When an investigation is underway, information is not shared with the broader community in the process outlined above. If in the course of the investigation, threat information is identified as needing to be shared, it is sanitized and placed in an analytic report and bulletin and disseminated to the appropriate audience. The products they produce may be disseminated through entities in other categories.

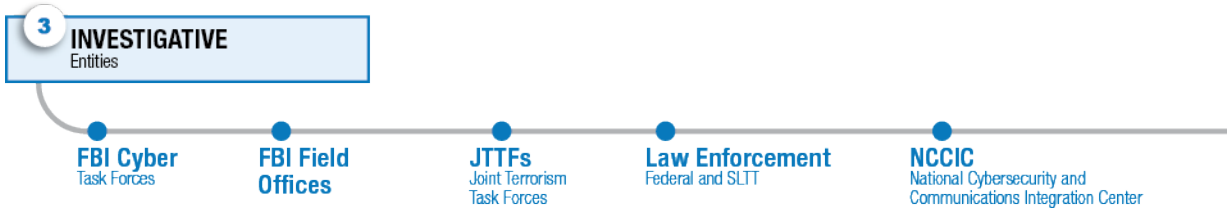


Figure 7: Investigative Entities

[45] For example, Joint Counterterrorism Assessment Team (JCAT) members are SLTT first responders and public safety professionals from around the country, working side-by-side with Federal intelligence analysts from the National Counterterrorism Center (NCTC), DHS, and the FBI to research, produce, and disseminate counterterrorism intelligence. The mission of JCAT is to improve information sharing and enhance public safety. JCAT collaborates with other members of the IC to research, produce, and disseminate counterterrorism intelligence products for Federal and SLTT government agencies and the private sector, and advocates for the counterterrorism intelligence requirements and needs of these partners throughout the IC.

2.2.4 Owners and Operators Operations Centers

Owners and operators security operations centers are run by individual critical infrastructure entities and are typically focused on monitoring and protecting that entity's assets. However, functions vary greatly between entities and some may share threat information with other entities in their sector, geographical area, etc.

2.2.5 Partnerships, Alliances, and Councils

Partnerships, alliances, councils, and associations, among other responsibilities, promote collaboration and dialogue among members and often provide information-sharing mechanisms (e.g., portals, tools, and briefings) for their members' use. These entities are often called upon for subject-matter expertise and/or leveraged to get threat information out quickly to their members during heightened threat environments or during an incident.

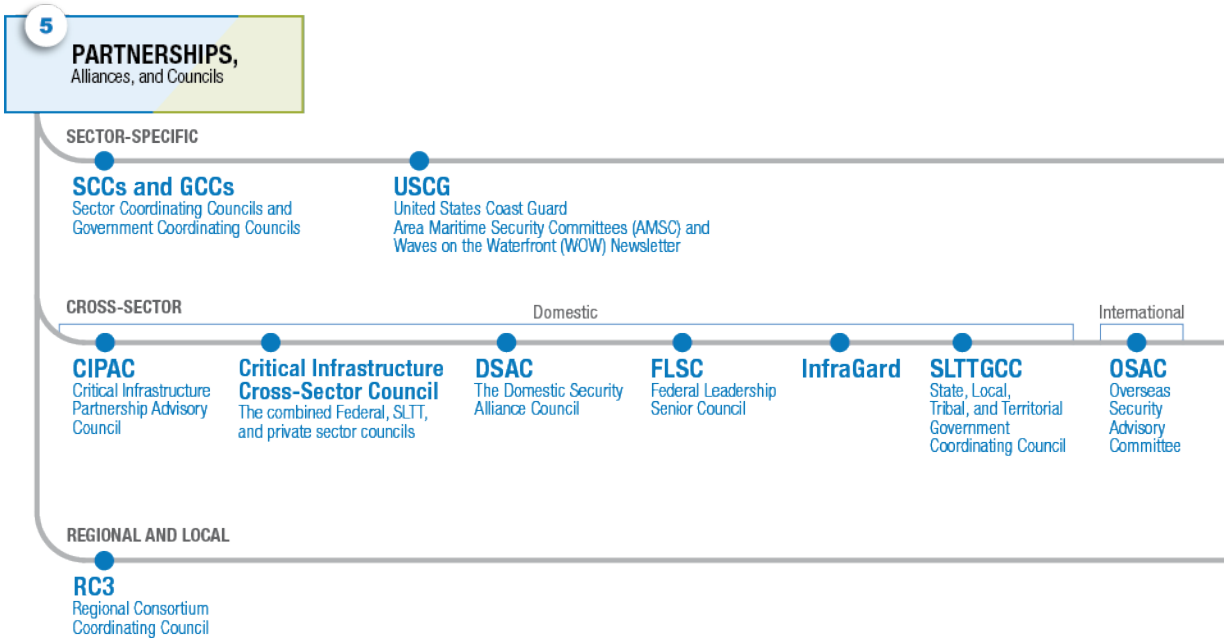


Figure 8: Partnerships, Alliances, and Councils

SECTION 3

Threat Information Sharing Entity Descriptions

The threat information-sharing entities listed in this section are those identified during the Framework development process as having a role in the threat information-sharing process described in Section 2. Other relevant entities that are not included in Section 3 are listed in Appendices A and B, though the Appendices do not contain a comprehensive list of every entity which shares threat information. The entities themselves drafted these descriptions based on a standard questionnaire.

The Domestic Security Alliance Council (DSAC)	
Category:	Partnerships, Alliances, and Councils – Cross-Sector – Domestic
General Description:	DSAC is an FBI-led partnership between DHS, the Federal Government, and U.S. Fortune 500 companies to strengthen national security and mitigate risk to the private sector through collaboration and information sharing. DSAC membership covers 13 of the 16 critical infrastructure sectors (Dams, Nuclear, and Government Facilities Sectors are not currently covered). Information provided to DSAC membership is for DSAC membership only, as agreed by each member via the DSAC Membership Charter.
Functions, Products, and Services Relevant to the Critical Infrastructure Community (specific to DSAC membership):	• Through its members-only portal, DSAC disseminates timely, relevant, and actionable intelligence that helps protect our Nation's critical infrastructure from terrorists, criminals, and other individuals or groups who pose risk. • It creates bridges between the private sector and local FBI Field Offices, in an effort to foster meaningful dialogue about the risks each company faces individually, what risks may be trending locally or within a particular business sector, and how the threat might play out on a national level. • In addition to its members-only portal, DSAC offers: ◦ Domestic Security Executive Academy (for DSAC member company Chief Security Officers [CSOs])[46] ◦ Integrated Analyst Symposia (for DSAC member company analysts)[47] ◦ Annual DSAC Conference (for DSAC member company CSOs)[48] ◦ Networking opportunities with other DSAC Members
Contact the DSAC if:	• You are a U.S. Fortune 500 company and would like to seek membership • As a DSAC member, you wish to obtain resources, including indicators, advisories, reports, intelligence products, and training • As a DSAC member, you wish to share trends; tactics, techniques, and procedures (TTPs); or best practices
How to Connect:	For the DSAC website and secure portal access request, go to http://www.dsac.gov/.
The DSAC in Action:	On December 11, 2015, DSAC hosted a webinar for its members to provide information from FBI, DHS, the Homeland Security Investigations (HSI), and owners and operators on potential counterterrorism, criminal, and cyber threats surrounding Super Bowl 50 and related events; an overview of the Super Bowl week schedule of events and venues; and an overview of security operations and interagency security planning. The webinar utilized HSIN Connect to allow participants to join via mobile device or a desktop computer.

[46] The Domestic Security Executive Academy (DSEA) is a strategic engagement program to incorporate chief security officers (CSOs) and Federal law enforcement senior executives. Held twice yearly at the FBI Academy in Quantico, Virginia, the DSEA is a one-week program. Participants include CSOs, law enforcement executives, and FBI Field Office Special Agents in Charge. The DSEA is designed to provide executive level training and enable attendees to share methodologies and best practices.

[47] The Integrated Analyst Symposium (IAS) training program is a four-day series designed to provide analysts with a basic working knowledge of structured analysis. Through the use of lectures and small group exercises, students receive instruction on Structured Analytic Techniques (SAT) to evaluate and prepare analytical assessments. The IAS curriculum begins with basic terminology, the intelligence cycle, and the sorting of information. Participants then transition to a track focused on biases and mindsets, critical thinking, and the practical application of SATs. Training concludes with an applied exercise in analysis, where students receive a sample scenario and must identify the risk, determine the extent of the problem, analyze available data, and develop several courses of action to be briefed to leadership.

[48] The DSAC Conference features panels and discussions with top FBI, DHS, and private sector leaders. The discussions cover a variety of modern concerns facing the government and private industry, from cybersecurity, to insider threats, to international kidnapping.

FBI Field Offices	
Category:	Local and Regional Information-Sharing Hubs; and Investigative Entities
General Description:	The FBI operates 56 field offices, located in major metropolitan areas across the U.S. and Puerto Rico, where the FBI carries out investigations, assesses local and regional crime threats, and works closely with Federal and SLTT partners on cases and operations. As the lead investigative agency on terrorism and counterintelligence (per Executive Order 12333), all terrorism and counterintelligence threats should be reported to your nearest FBI field office either directly or through local authorities (including fusion centers).
Functions, Products, and Services Relevant to the Critical Infrastructure Community:	The FBI has many private sector programs all around the country. In addition to DSAC (highlighted above) and InfraGard (highlighted below), the FBI also has outreach coordinators in each of its 56 field offices and online resources for these programs and more: • Active Shooter: https://www.fbi.gov/about-us/office-of-partner-engagement/active-shooter-incidents • Campus Liaison: https://www.fbi.gov/news/stories/2009/august/campussecurity_080409 • Community Outreach program: https://www.fbi.gov/about-us/partnerships_and_outreach/community_outreach • Counterintelligence Strategic Partnership: https://www.fbi.gov/about-us/partnerships_and_outreach/investigate/counterintelligence/strategic-partnerships • Cyber Forensics and Training Alliance: https://www.fbi.gov/news/stories/2011/september/cyber_091611 • Insider Threat brochure: https://www.fbi.gov/about-us/investigate/counterintelligence/insider_threat_brochure • Summary of public-private information-sharing partnerships: https://www.fbi.gov/about-us/partnerships_and_outreach/ • Terrorism: https://www.fbi.gov/about-us/investigate/terrorism • Weapons of Mass Destruction: https://www.fbi.gov/news/stories/2007/march/wmd030507 • The FBI adheres to the ODNI Intelligence Community Directive 191, Duty to Warn, signed 7/21/2015: http://www.dni.gov/files/documents/ICD/ICD_191.pdf
Contact Your Local FBI Field Office to:	• Report all terrorism and counterintelligence threats • Report a cyber incident • Receive a product or service as outlined above
How to Connect:	You can directly report threats and incidents and contact your nearest FBI field office as follows: • Online: https://www.fbi.gov/report-threats-and-crime • Contact your nearest FBI field office at https://www.fbi.gov/contact-us/field or nearest international office at https://www.fbi.gov/contact-us/legat • To report suspicious activity involving chemical, biological, or radiological materials, call (toll-free) 855-TELL-FBI (855-835-5324) • Report an online scam or email hoax by filing a complaint online with the Internet Crime Complaint Center at http://www.ic3.gov/complaint/default.aspx or by using the online Tips and Public Leads form at https://tips.fbi.gov/ • To provide information on select major cases, call the Major Case Contact Center at 1-800-CALL-FBI (1-800-225-5324)
FBI Field Offices in Action:	The Navy Yard shootings in Washington, D.C., the Boston Marathon bombings, and Hurricane Sandy are examples of the types of major cases and catastrophic events where the FBI wants to hear from the public so the FBI can act quickly to provide assistance, protection, and prevention to threats to this Nation and its public.

Federal Sector-Specific Operations Centers	
Category:	National Information-Sharing Hubs – Many of which interact directly with Owners/Operators[49]
General Description:	Federal departments and agencies use their organizational operation/watch centers to meet internal information-sharing requirements relating to critical infrastructure security and resilience situational awareness. The roles and responsibilities of relevant Federal operations centers, as well as points of contact, are listed in Appendix A.
Functions, Products, and Services Relevant to the Critical Infrastructure Community:	• Provide situational awareness and share information in the event of a natural disaster, act of terrorism, or other disaster • Serve as a day-to-day Federal interface for the dynamic prioritization, collaboration, and coordination of sector-specific activities • Protect critical infrastructure and ensure government continuity through a risk management process based upon Interagency Security Committee standards and the National Infrastructure Protection Plan (NIPP) • Provide incident prevention and/or interdiction, threat mitigation, and incident coordination and management • Facilitate the continuity of operations/government, disaster policy, planning, support, and operational coordination; and special security programs
Contact Your Federal Operations Center:	These operations centers often communicate directly with owners and operators within their sector, though some communicate primarily during disasters.
Further Information:	See Appendix A for a list of the Federal Sector-Specific Operations Centers, their roles, websites and contact information.

[49] Federal Sector-Specific Operations Centers have varying operational models. Some primarily support their internal agency needs and do not interact directly with critical infrastructure owners and operators, however many do. See entity descriptions in Appendix A for further information.

Fusion Centers (State and Major Urban Area Fusion Centers)

Category:	Local and Regional Information-Sharing Hubs
General Description:	State and major urban area fusion centers are owned and operated by State and local entities and serve as the primary focal points within the State and local environment for the receipt, analysis, gathering, and sharing of threat-related information among Federal, SLTT, and private sector partners. Fusion centers provide multidisciplinary all-crimes and all-hazards expertise and situational awareness to help inform decision-making at all levels of government and throughout the private sector. They conduct analyses and facilitate information sharing, while assisting law enforcement and homeland security partners in preventing, protecting against, and responding to criminal activity, terrorism, and hazards—both manmade and natural.
Functions, Products, and Services Relevant to the Critical Infrastructure Community:	Fusion center products help customers understand the local implications of national intelligence, thus helping State and local officials better protect their communities and helping private sector partners protect their facilities and operations. These products are often provided to private sector partners directly from the fusion center, and many products may also be accessible via the Homeland Security Information Network – Critical Infrastructure (HSIN-CI) community of interest, which facilitates the sharing of products and information with all participating partners: https://www.dhs.gov/hsin-ci. Depending on their focus and the individual needs of their customers, fusion centers may provide several types of products and services: • **Responses to Requests for Information** – Solicitation for specific information from a customer • **Situational Awareness Products** – Information regarding developing events or incidents • **Bulletins** – Information concerning criminal threats and incidents and/or potential terrorist threats • **Intelligence Warning Bulletins** – Credible reports or analytic indications of a specific or imminent threat • **Advisory Notifications** – Information regarding regional cyber and physical security incidents and developing criminal trends and tactics • **Formal Reports** – Formalized periodic and situational reports • **Threat Assessments** – Detailed information about the nature of a particular threat and current and future trends • **Risk Assessments** – Comprehensive assessments based on analyses of threats, vulnerabilities, and consequences • Classified Threat Briefings
Contact the Fusion Center in Your Area to:	• Obtain information about available products and services and how to access them • Join distribution lists or online information sharing portals • Share Suspicious Activity Reporting (SAR) information with your area fusion center for terrorism and other related criminal activity (free online SAR training for the private sector and other sectors is available at https://nsi.ncirc.gov/training_online.aspx) • Share tips and leads for non-terrorism related crimes (Note: not all fusion centers focus on all crimes) • Participate in fusion center governance or serve on an advisory body • Connect with Federal field personnel. In many cases, the FBI, DHS, and other agencies with field personnel deploy or co-locate personnel at fusion centers. For example, DHS I&A deploys Regional Directors, Intelligence Officers, and Reports Officers to every fusion center. Occasionally, IP's Protective Security Advisors (PSAs) are also co-located in fusion centers.
How to Connect:	• For more information on the fusion center in your area, please visit https://www.dhs.gov/contact-fusion-centers • You can engage through deployed personnel from DHS, including I&A Regional Directors, Intelligence Officers (IOs), and Reports Officers; as well Security Advisors • Contact a fusion center's liaison officer responsible for private sector outreach.
Fusion Centers in Action:	Fusion centers have a network of contacts throughout their area of responsibility. This network allows fusion centers to reach out into the community to gather information that may help law enforcement to solve crimes or prevent terrorist attacks. One example is the case of a planned terrorist attack by a Denver airport shuttle driver. A fusion center facilitated information gathering from supply stores all over Colorado. The analysis of this collected information helped prevent the attack and facilitate the arrest of a terrorist. Please also see the use cases in Section 4. For additional use cases, see the Fusion Center Success page on DHS.gov: https://www.dhs.gov/fusion-center-success-stories.

Information Sharing and Analysis Centers (ISACs)	
Category:	National Information-Sharing Hubs – Interacts Directly with Owners/Operators; and Partnerships, Alliances, and Councils – Sector-Specific
General Description:	ISACs are sector-specific, private, trusted member-driven entities established by critical infrastructure owners and operators to collect, analyze, and disseminate timely and actionable threat information to their members, to other sectors, and to government entities. ISACs also provide members with tools and best practices to mitigate risks and enhance resiliency. Depending on the sector, ISACs can operate on a free or paid-membership basis.
Functions, Products, and Services Relevant to the Critical Infrastructure Community:	• Each ISAC employs its particular sector knowledge and expertise to: • Save members time and effort by serving as a clearinghouse for government and private information, helping members identify risks, prepare for emergencies, and secure sector-specific critical infrastructure • Research and analyze the information it has received in order to validate the accuracy of the information and the severity of any threats and to recommend actions • Filter information for sector and regional specifications • Communicate threat warnings and incident reports through eNewsletters, threat notification emails, or other mediums ◦ Provide members with tools for identifying and managing risks ◦ Foster cooperation and communication among members by using a secure trusted network to support their mutual benefit
Contact Your Sector's ISAC to:	• Learn more about what your sector's ISAC provides • Join your sector's ISAC • Report a sector-specific incident
How to Connect:	• See below for a list of ISACs by sector/industry and their websites • The National Council of ISACs website provides information about cross-sector collaboration and more information on each of the ISACs: www.nationalisacs.org
ISACs in Action:	On January 1, 2016, expert analysts at Electricity ISAC (E-ISAC) released an unclassified comprehensive Cyber Event Report to electricity sector members detailing certain December 2015 events in Ukraine. This open source compilation product described real world events, gave detailed background information, applied sector-specific analysis addressing impact and mitigation considerations for the sector and others, and offered technical information. A subsequent cross sector and federal partners analyst meeting was also hosted at E-ISAC for collaborative security partner organizations.
ISAC Websites:	• Aviation (A-ISAC): www.a-isac.com • Communications (COMM-ISAC):[50] http://www.dhs.gov/national-coordinating-center-communications • Defense Industrial Base (DIB-ISAC): http://dibisac.net/ • Downstream Natural Gas (DNG-ISAC): www.dngisac.com/ • Electricity (E-ISAC): www.eisac.com • Emergency Services (EMR-ISAC): www.usfa.fema.gov/fireservice/emr-isac • Financial Services (FS-ISAC): www.fsisac.com • Healthcare (NH-ISAC): www.nhisac.org • Information Technology (IT-ISAC): www.it-isac.org • Multi-State (MS-ISAC): www.msisac.org • Nuclear (NEI): www.nei.org/ • Oil and Natural Gas (ONG-ISAC): www.ongisac.org/ • Public Transit (PT-ISAC): www.surfacetransportationisac.org • Real Estate (RE-ISAC): www.reisac.org • Research and Education Networking (REN-ISAC): www.ren-isac.net • Retail Cyber Intelligence Sharing Center (RCS-ISAC): http://r-cisc.org/ • Supply Chain (SC-ISAC): www.sc-isac.org • Surface Transportation (ST-ISAC): www.surfacetransportationisac.org • Water (WaterISAC): www.waterisac.org • Healthcare Ready www.healthcareready.org

[50] The NCCIC's National Coordinating Center for Communications (NCC) serves as the COMM-ISAC.

Information Sharing and Analysis Organizations (ISAOs)	
Category:	Local, Regional, and National Information-Sharing Hubs – Interacts Directly with Owners/Operators; and Partnerships, Alliances, and Councils
General Description:	ISAOs are a broader category of private information-sharing organizations, which include ISACs. Some organizations do not fit neatly within an established sector or have unique needs. Those organizations that cannot join an ISAC but have a need for threat information could benefit from membership in an ISAO, for example places of worship. The establishment of new ISAOs allows communities of interest to share threat information with each other and existing public and private entities on a voluntary basis to create deeper and broader networks of threat information sharing across the Nation. President Obama issued an Executive Order directing DHS to encourage the development of new ISAOs, and the ISAO Standards Organization (ISAO-SO), led by the University of Texas at San Antonio, has been working with the critical infrastructure community to identify a common set of voluntary standards for the creation and functioning of ISAOs since its establishment on October 1, 2015. These standards are one of the key distinctions between ISAOs and ISACs.
Functions, Products, and Services Relevant to the Critical Infrastructure Community:	• Each ISAO employs its particular sector knowledge and expertise to: • Serve as a clearinghouse for government and private threat information that helps members identify risks, prepare for emergencies, and secure critical infrastructure • Research and analyze information received to validate accuracy and severity and recommend actions • Filter information for sector and regional specification • Communicate threat warnings and incident reports through eNewsletters, threat notification emails, or other mediums ◦ Provide tools for identifying and managing risks ◦ Foster cooperation and communication among members to their mutual benefit ◦ Expand sharing relationships beyond traditional critical infrastructure sectors, for example, places of worship
Contact Relevant ISAOs or the ISAO Standards Organization (ISAO-SO) to:	• Learn more about what relevant ISAOs provide • Join an ISAO • Start a new ISAO • Report a sector-specific incident
How to Connect:	• ISAOs are a new type of entity and at the time of writing do not fully exist yet • Learn more about ISAOs at http://www.dhs.gov/isao • Get the ISAO fact sheet at https://www.whitehouse.gov/the-press-office/2015/02/12/fact-sheet-executive-order-promoting-private-sector-cybersecurity-inform • To participate in developing or to access the standards and guidance for starting new ISAOs, see the ISAO Standards Organization at https://www.isao.org or email contact@isao.org

InfraGard	
Category:	Partnerships, Alliances, and Councils – Cross-Sector – Domestic
General Description:	InfraGard is a public-private partnership between the FBI and over 40,000 vetted members of the private sector, representing all 16 critical infrastructure sectors. It is an association of members with subject matter expertise who represent businesses, academic institutions, and government at all levels, and State and local law enforcement agencies, as well as other participants dedicated to providing multidirectional sharing of information, intelligence, strategy, and expertise to prevent hostile acts against the U.S. There are over 80 InfraGard chapters nationwide.
Functions, Products, and Services Relevant to the Critical Infrastructure Community:	• InfraGard members enjoy access to: • InfraGard's Secure Web Portal for information sharing • iGuardian, the FBI's cyber incident reporting tool designed specifically for the private sector • A comprehensive suite of sensitive, unclassified FBI and other threat intelligence projects and daily news feeds from many sources • FBI and DHS threat advisories, intelligence bulletins, analytical reports, and vulnerability assessments in real time ◦ Member events hosted by Local InfraGard Member Alliances (IMAs) that include FBI and other government agency presentations and provide in-person opportunities for threat briefings and information sharing in a trusted environment ◦ Provision of a venue if needed to report and discuss threats ◦ Training
Contact InfraGard to:	• Become a member (You must be a U.S. citizen and 18 years of age or older) • Request a briefing or training with your local IMA • Report a cyber intrusion through InfraGard's secure portal, iGuardian (InfraGard members only) ◦ Anyone can report a cyber incident on the FBI's Internet Crime Complaint Center (IC3): http://www.ic3.gov
How to Connect:	• Membership application and access to InfraGard's Secure Web Portal: www.infragard.org • For general questions relating to membership, please contact questions@infragardmembers.org
InfraGard in Action:	Beginning February 27, 2015, Malware Investigator was made available to the private sector for the first time through the InfraGard portal for members. Malware Investigator uses an extensive combination of dynamic and static analysis tools to understand how malware samples interact within various types of host environments. The platform also correlates samples and enables collaboration with others, if desired, to "connect the dots" between cyber events. The system, built in cooperation with Federal partners, is an extension of an internal malware analysis tool that the FBI created for its own use in 2011. Private partner access to Malware Investigator benefits both private sector partners and the FBI by strengthening strategic partnerships through collaboration that will ultimately assist in understanding and combating malware threats.

Investigative and/or Intelligence Entities (Non-Public-Facing)	
Category:	Investigative Entities
General Description:	Behind many of the publically facing Federal threat information-sharing entities are many other non-public-facing Federal investigative bodies who share information across the Federal Government.
Functions, Products, and Services Relevant to the Critical Infrastructure Community:	Intelligence products or derivatives of their products are shared with owners and operators through other entities listed in this Framework.
Contact:	These operations centers generally do not communicate directly with owners and operators.
How to Connect:	For more information, see the Intelligence Guide for First Responders by the Joint Counterterrorism Assessment Team (JCAT): http://www.nctc.gov/jcat/docs/Intelligence_Guide_for_First_Responders.pdf
Select Investigative and/or Intelligence Entities (Non-Public-Facing):	**Joint Terrorism Task Force (JTTF):** JTTFs serve as the coordinated "action arms" for federal, state, and local governments to investigate terrorist threats in specific U.S. geographic regions. FBI serves as the lead agency to oversee JTTFs. The mission of the JTTF is to use the collective resources of the member agencies to prevent, preempt, deter, and investigate terrorist acts that affect U.S. interests; to disrupt and prevent terrorist acts; and to apprehend individuals who may commit or plan to commit such acts. To further this mission, the JTTF facilitates information sharing among JTTF members. More than 500 State and local agencies participate in JTTFs nationwide, and federal representation includes participants from the IC, DHS, and the Departments of Defense, Justice, Treasury, Transportation, Commerce, Energy, State, and the Interior, among others.[51] **National Counterterrorism Center (NCTC):** NCTC serves as the primary organization in the Federal Government for integrating and analyzing all intelligence pertaining to terrorism possessed or acquired by the Federal Government (except purely domestic terrorism); serves as the central and shared knowledge bank on terrorism information; provides all-source intelligence support to government-wide counterterrorism activities; and establishes the integration, dissemination, and use of, terrorism information.[52] It also produces the NCTC Counterterrorism (CT) Digest, a compendium of international and domestic news focusing on counterterrorism information. It is available on HSIN-CI, InfraGard, and DSAC. CT Digest also contains assessments from seasoned analysts and first responders. **Terrorist Screening Center (FBI-TSC):** Born out of the events of 9/11 and created in 2003, the TSC maintains the U.S. government's consolidated Terrorist Watchlist—a single database of identifying information about those known or reasonably suspected of being involved in terrorist activity. By supporting the ability of front-line screening agencies to positively identify known or suspected terrorists trying to obtain visas, enter the country, board aircraft, or engage in other activity, the consolidated Terrorist Watchlist is one of the most effective counterterrorism tools for the U.S. government.

[51] National Counterterrorism Center, JCAT Intelligence Guide for First Responders, http://www.nctc.gov/jcat/docs/Intelligence_Guide_for_First_Responders.pdf (accessed June 21, 2016).

[52] National Counterterrorism Center, Who We Are, http://www.nctc.gov/whoweare.html (accessed June 21, 2016).

Local and State Law Enforcement Operations Centers	
Category:	Local and Regional Information-Sharing Hubs; and Investigative Entities
General Description:	In an emergency always call 9-1-1 to contact your local or State law enforcement authorities. Law enforcement information-sharing systems for threat and intelligence information varies by community. Some major cities have built trusted, established information-sharing relationships and mechanisms, while in others owners and operators may find it difficult to regularly communicate with police departments about suspicious activity. New York Police Department (NYPD) Shield, for example, sponsors email notifications, web briefings, and periodic in-person briefings. Their staff of analysts are dedicated specifically to terrorism prevention and pushes information out to the private sector, and is at times faster at getting information analyzed and out than HSIN-CI. However, this network is only accessible for critical infrastructure in New York City.[53] Another example is the Regional Information Sharing Systems' (RISS) Automated Trusted Information Exchange (ATIX) whose community groups include law enforcement, emergency management, government, as well as an increasing number of groups over-lapping critical infrastructure sectors, including water and power utilities, transportation, agriculture, chemical manufacturing, private security, environmental protection, banking and finance, and hospitality.
Functions, Products, and Services Relevant to the Critical Infrastructure Community:	• Emergency response to and support for immediate physical and cyber threats and incidents • Threat information sharing • Investigation into incidents
Contact Your Local Law Enforcement Operations Center to:	• Explore opportunities to collaborate and share local threat information • Sign up for threat information notifications and other services that may be available
How to Connect:	• Contact your local law enforcement through their non-911 phone number • Example web portal: NYPD Shield: http://www.nypdshield.org/public/ • RISS ATIX: More information, including Regional Centers' contact information, can be found in the brochure located at www.riss.net/Resources/ATIX

[53] National Infrastructure Advisory Council, *Intelligence Information Sharing: Final Report and Recommendations*, January 2012, http://www.dhs.gov/sites/default/files/publications/niac-intel-info-sharing-final-report-01-10-12-508.pdf (accessed June 21, 2016), p. D-10.

National Cybersecurity and Communications Integration Center (NCCIC)

Category:	National Information-Sharing Hubs – Interacts Directly with Owners/Operators; and Investigative Entities
General Description:	The NCCIC serves as a focal point for cybersecurity incident coordination, information sharing, and incident response across the Federal civilian government and provides cybersecurity and National Security/Emergency Preparedness communications assistance to public and private sector partners. These services include protection, prevention, detection, mitigation, response, and, in the case of communications, restoration services. NCCIC partners include all Federal departments and agencies, SLTT governments, the private sector, the intelligence community, law enforcement, and international entities. The NCCIC is composed of four branches: the U.S. Computer Emergency Readiness Team (US-CERT), the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), the National Coordinating Center for Communications (NCC), and Operations and Integration, which includes National Cybersecurity Assessment and Technical Services (NCATS). For more information on each branch, see https://www.dhs.gov/cyber-incident-response.
Functions, Products, and Services Relevant to the Critical Infrastructure Community:	• Information sharing: ◦ In-person information sharing on the NCCIC watch floor ◦ Bilateral exchange of actionable cyber threat indicators via two secure web-based portals and through a secure machine-to-machine interface called the Automated Indicator Sharing (AIS): ◦ The Cyber Information Sharing and Collaboration Program (CISCP) ◦ Automated sharing and receipt of cyber threat indicators in a machine-readable format known as the Structured Threat Information eXpression (STIX) ◦ As-needed information sharing via standing groups ◦ Broad dissemination of actionable alerts, briefings, advisories, and bulletins to the community through multiple venues, including emails, two secure web-based portals, ISACs, and SSAs • Coordinate and manage the national response to significant cyber incidents and provides direct incident assistance to victims of a cyberattack, upon request • Coordinates risk reduction efforts by working directly with owners and operators to provide: ◦ No-cost, onsite, in-depth cybersecurity assessments of critical infrastructure assets that help owners and operators prepare for and protect against cyberattacks ◦ Free training to improve asset owners' cybersecurity skills and practices ◦ Analysis of malicious activity ◦ Incident response services • Facilitation of working groups that exchange ideas on mitigation techniques
Contact the NCCIC to:	• Report a suspected or confirmed cyber incident[54] • Obtain cyber protection resources, including indicators, threat advisories, reports, and malware digests tailored to critical infrastructure owners and operators • Obtain strategies on prevention, protection, and mitigation • Request and schedule a no-cost, onsite cybersecurity assessment for your control systems assets, resource and availability permitting • Learn how to submit cyber threat indicators to DHS that can be shared with other private sector entities to improve their network defense posture, including use of the Automated Indicator Sharing (AIS): www.us-cert.gov/ais

[54] For more information on when, what, and how to report cyber incidents to the Federal Government, see https://www.dhs.gov/sites/default/files/publications/Law%20Enforcement%20Cyber%20Incident%20Reporting.pdf (accessed June 21, 2016).

National Cybersecurity and Communications Integration Center (NCCIC)

How to Connect:	• To report an incident, go to https://www.us-cert.gov/forms/report, email nccicustomerservice@hq.dhs.gov, or call 888-282-0870 • To report cyber incidents targeting industrial control systems, email ics-cert@hq.dhs.gov or call 877-776-7585 • To receive NCCIC alerts, signup at https://www.us-cert.gov/mailing-lists-and-feeds • To participate in automated indicator sharing, go to https://www.us-cert.gov/ais • To request various cybersecurity assessments, go to https://www.us-cert.gov/ccubedvp/assessments or https://ics-cert.us-cert.gov/Assessments, or email ncats_info@hq.dhs.gov • To make a secure portal access request: ◦ US-CERT Cobalt Compartment (enterprise systems) – To request access, send an email to NCCIC_Partnership@hq.dhs.gov with the subject line, "Request access to Cobalt Compartment" ◦ ICS-CERT Control System Compartment (ICS owners and operators) – To request access, send an email to ics-cert@hq.dhs.gov with the subject line, "Request access to Control System Compartment" ◦ For more information, go to https://www.dhs.gov/national-cybersecurity-and-communications-integration-center
NCCIC in Action:	See the Havex/BlackEnergy use case in Section 4.1 on page 45 to see how the NCCIC shared ICS malware threat information with owners and operators through briefings and alerts.

National Infrastructure Coordinating Center (NICC)	
Category:	National Information-Sharing Hubs – Interacts Directly with Owners/Operators
General Description:	The NICC is one of two national infrastructure center designated by the Secretary of Homeland Security and, as directed by PPD-21, and serves as the focal point for critical infrastructure partners to obtain situational awareness and integrated, actionable information that can be used to protect the physical aspects of critical infrastructure.
Functions, Products, and Services Relevant to the Critical Infrastructure Community:	• Serves as the private sector's entry point to the security and resilience programs led and coordinated by the DHS National Protection and Programs Directorate's Office of Infrastructure Protection (IP). For more information on how the private sector collaborates with IP, please visit https://www.dhs.gov/topic/critical-infrastructure-security. • Serves as the administrator of the critical infrastructure community on the Homeland Security Information Network – Critical Infrastructure (HSIN-CI), the trusted network for homeland security mission operations to share sensitive but unclassified (SBU) information. HSIN-CI is the primary system through which private sector owners and operators, DHS, and other Federal, State, and local government agencies collaborate to protect the Nation's critical infrastructure. For more information on HSIN-CI, please visit https://www.dhs.gov/hsin-ci. • Processes and posts Suspicious Activity Reports (SAR). For more information on the SAR initiative, please visit http://www.dhs.gov/how-do-i/report-suspicious-activity. • Conducts critical infrastructure stakeholder teleconference calls through IP.
Contact the NICC to:	• Receive, submit, and discuss timely, actionable, and accurate information regarding critical infrastructure • Maintain a direct, trusted channel with DHS and other vetted sector stakeholders • Communicate information pertaining to threats, vulnerabilities, security, and response and recovery activities affecting sector and cross-sector operations
How to Connect:	• Report physical infrastructure incidents or request information by emailing NICC@hq.dhs.gov or calling (202) 282-9201 • Request access to HSIN-CI, by submitting an email to hsinci@hq.dhs.gov with: ◦ First and last name ◦ Title ◦ Employer ◦ Valid email address ◦ Brief written justification for access, including the critical infrastructure sector(s) or mission you support • A validating authority will review your membership application to determine your suitability for admission. If your application is approved, you will be sent an email with instructions on how to log onto HSIN for the first time.
The NICC in Action:	In May 2015, the NICC posted a series of Joint Intelligence Bulletins, Field Analysis Reports, DHS Terrorism Reports, and other notification and assessment documents to HSIN-CI regarding the increased threat situation and the need for vigilance following the terrorism incident in Garland, TX. These posts included audio recording from the Critical Infrastructure Stakeholder Teleconference Call, which provided the government and owners and operators with a forum to share incident- and threat-specific information. IP leads the coordination and execution of Critical Infrastructure Stakeholder Teleconference Calls.

Office of Intelligence and Analysis (DHS I&A)	
Category:	National Information-Sharing Hubs – Interacts Directly with Owners/Operators
General Description:	DHS I&A is a member of the IC and plays a supporting role in defending our Nation's critical infrastructure and sharing related protected information. Through its Field Personnel—including Regional Directors, Intelligence Officers, and Reports Officers and Intelligence Analysts—I&A collects, analyzes, and disseminates threat information that is specific to critical infrastructure in support of the Department's national security mission.
Functions, Products, and Services Relevant to the Critical Infrastructure Community:	I&A employs its intelligence and information sharing knowledge and expertise to: • Collect, analyze, and disseminate intelligence and information about threats to critical infrastructure • Provide products and threat briefings, in coordination with the PSAs who are pertinent to threats to critical infrastructure • Provide incident response support to other key DHS responders
Contact Your Local I&A Field Personnel to:	• Coordinate critical infrastructure-related threat intelligence and information sharing • Request a threat briefing in conjunction with PSAs
How to Connect:	Email Field_Operations@hq.dhs.gov for information about how to contact your nearest I&A representative
I&A in Action:	Please see the use cases in Section 4.

Overseas Security Advisory Council (OSAC)	
Category:	Partnerships, Alliances, and Councils – Cross-Sector – International
General Description:	OSAC was created to promote open dialogue between the U.S. Government and the American private sector on security issues abroad. Today, over 4,000 U.S. private sector organizations rely upon OSAC for timely and unbiased safety and security-related information. OSAC shares information through a network of constituent organizations, including for-profit companies, nongovernmental organizations (NGOs), and faith-based organizations; academic institutions; 14,000 registered website users; and 149 country councils across the world.
Functions, Products, and Services Relevant to the Critical Infrastructure Community:	There are numerous products available on OSAC.gov, OSAC's public-facing information portal: • **All Consular Messaging**, including Security Messages, Travel Advisories, etc. • **Crime and Safety Reports**, providing a primer on a location's security environment • **Newsletters**, providing constituents timely security-related news and events updates • **OSAC Analytic Reports**, thematic, ad-hoc reports on security-related topics • **Resource Library**, including compiled reference materials related to global security • **Training**, including an eight module security awareness program OSAC also provides several mechanisms in outreach and engagement efforts for members of the U.S. private sector to exchange information amongst themselves, including virtual support. These efforts include targeted, security-focused listservs and in-person meetings via country councils at U.S. embassies and consulates. OSAC's staff also manages several regionally focused councils and sector-specific working groups. In accordance with the U.S. Department of State's No Double Standard policy (7 FAM 052),[55] OSAC coordinates Duty to Warn notifications of specific, credible threats of death, serious physical injury, or kidnapping that target identified U.S. private sector organizations. In cases where threat information is non-specific in nature, OSAC works with the Bureau of Consular Affairs to release consular messaging to warn the broader U.S. community.
Contact OSAC to:	• Become a constituent organization • Consult with OSAC's staff of regional security professionals on international threats facing U.S. private sector organizations • Subscribe to OSAC alerts, newsletters, and analytic reports
How to Connect:	• Social Media: @OSACState on Twitter.com • General Information: ◦ https://www.osac.gov ◦ Send OSAC an email at the Contact Us page: https://www.osac.gov/Pages/ContactUs.aspx ◦ Phone: 571-345-2223 • Emergency Duty Officer (Emergency Situations Only): ◦ Phone: 202-309-5056 ◦ Email: osac_risc@state.gov
OSAC in Action:	In FY 2015, OSAC global security coordinators identified over 113 specific and credible threats to U.S. private sector organizations operating around the world. Duty to Warn threat notifications were provided to the domestic headquarters of each organization and foreign-based representatives through the Bureau of Diplomatic Security's regional security office at U.S. embassies and consulates. These notifications were coordinated with partners in the U.S. intelligence and law enforcement communities to ensure the accuracy and utility of the information provided to mitigate potential threats.

[55] "In administering the Consular Information Program, the Department of State applies a 'no double standard' policy to important security threat information, including criminal information. Generally, if the Department shares information with the official U.S. community, it should also make the same or similar information available to the non-official U.S. community if the underlying threat applies to both official and non-official U.S. citizens/nationals," (7 FAM 052.1).

Owners and Operators Operations Centers	
Category:	Owners and Operators Operations Centers
General Description:	Owner and Operator operations centers are run by individual critical infrastructure entities and typically focus on monitoring and protecting that entity's assets. However, due to the diverse nature of the security needs of each entity, operations and functions vary greatly between entities.
Functions, Products, and Services Relevant to the Critical Infrastructure Community:	• Receives and shares threat information, both internally and with ISACs and neighboring utilities • Manages all aspects of: ◦ Access control ◦ Security systems ◦ Emergency management ◦ Business continuity through use of Mission Mode ◦ Emergency notifications • Incident response
How to Connect:	• Informational sharing entities can contact individual owners and operators • External owners and operators generally do not connect with these centers except for possible neighboring relationships
Private Sector Operations and Watch Centers in Action:	See the Metcalf electric substation use case in Section 4.2 on page 50.

Protective Security Advisor (PSA) Program	
Category:	Entities with Critical Infrastructure Security and Resilience Program, Policy, and Mitigation Responsibilities (See Appendix C)
General Description:	The Office of Infrastructure Protection (IP), within the National Protection and Programs Directorate (NPPD) of DHS, operates the PSA Program. PSAs are security subject matter experts (SMEs) who engage with SLTT government mission partners and members of the private sector stakeholder community to protect the Nation's critical infrastructure. The PSA Program maintains a robust operational field capability, with Chief Protective Security and PSAs serving all 50 States and the U.S. territories. The RDs and PSAs serve as the link to DHS infrastructure protection resources; coordinate vulnerability assessments, training, and other DHS products and services; provide a vital link for information sharing in steady state and incident response; and assist facility owners and operators with obtaining security clearances.
Functions, Products, and Services Relevant to the Critical Infrastructure Community:	The PSAs have five mission areas that directly support the protection of critical infrastructure: • Plan, coordinate, and conduct security surveys and assessments – PSAs conduct voluntary, non-regulatory security surveys and assessments on critical infrastructure assets and facilities within their respective regions • Plan and conduct outreach activities – PSAs conduct outreach activities with critical infrastructure owners and operators, community groups, and faith-based organizations in support of IP priorities • Support National Special Security Events (NSSEs) and Special Event Activity Rating (SEAR) events – PSAs support Federal, State, and local officials responsible for planning, leading, and coordinating NSSE and SEAR events • Respond to incidents – PSAs plan for and, when directed, deploy to Unified Area Command Groups, Joint Operations Centers, Federal Emergency Management Agency Regional Response Coordination Centers, and/or State and local Emergency Operations Centers in response to natural or manmade incidents • Coordinate and support improvised explosive device awareness and risk mitigation training – PSAs work in conjunction with IP's Office for Bombing Prevention by coordinating training and materials to SLTT partners to assist them in deterring, detecting, preventing, protecting against, and responding to improvised explosive device threats
Contact Your Nearest PSA to:	• Receive, submit, and discuss timely, actionable, and accurate information regarding critical infrastructure • Maintain a direct, trusted channel with DHS and other vetted sector stakeholders • Communicate information pertaining to threats, vulnerabilities, security, and response and recovery activities affecting sector and cross-sector operations • Learn more about critical infrastructure protection resources, including training on topics such as active shooters, IEDs, and insider threats: https://www.dhs.gov/critical-infrastructure-training
How to Connect:	For more information or to contact your nearest PSA, please contact PSCDOperations@hq.dhs.gov
The PSA Program in Action:	Since 2005, PSAs have engaged government mission partners and members of the private sector stakeholder community to protect the Nation's critical infrastructure. To date in 2016, they have conducted hundreds of vulnerability assessments and security surveys. PSAs have supported the Security Assistance to Public Gatherings outreach campaign; and they have supported numerous special events to include Super Bowl 50 and Times Square New Year's Eve. PSAs provided incident response support activities to natural disasters (flooding, winter storms) and coordinated multiple training sessions including Active Shooter presentations and the Office for Bombing Prevention's Surveillance Detection Courses and IED Awareness/Bomb Threat Management Workshops.

Sector Coordinating Councils (SCCs)	
Category:	Partnerships, Alliances, and Councils – Sector-Specific
General Description:	Sector Coordinating Councils (SCCs) are self-organized, self-run, and self-governed councils consisting of owners and operators, their trade associations, vendors, and others to interact on a wide range of sector-specific strategies, policies, activities, and issues. SCCs serve as principal collaboration points between the government and owners and operators for critical infrastructure security and resilience activities. They are the private sector counterpart to the Government Coordinating Councils (GCCs).
Functions, Products, and Services Relevant to the Critical Infrastructure Community:	The SCCs coordinate and collaborate with organizations across the entire NIPP partnership structure, including sector-specific agencies (SSAs), related GCCs, the Critical Infrastructure Cross-Sector Council, the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC), the Regional Consortium Coordinating Council (RC3), and the Federal Senior Leadership Council, to address the entire range of critical infrastructure security and resilience policies and efforts for each sector. SCCs serve as a voice for the sector and represent principal entry points for the government to collaborate with the sector for critical infrastructure security and resilience activities. Other primary functions of an SCC may include: • Serving as a strategic communications and coordination mechanism between owners, operators, trade associations, suppliers, and the government during emerging threats or response and recovery operations, as determined by the sector • Identifying, implementing, and supporting appropriate information-sharing capabilities and mechanisms in sectors where no information-sharing structure exists • Encouraging representative sector membership • Participating in planning efforts related to the cyclical revision of the National Infrastructure Protection Plan (NIPP), the development and revision of Sector-Specific Plans (SSP), and the annual submission of sector activities to DHS • Facilitating efforts to ensure an inclusive organization and coordinating the sector's policy development regarding critical infrastructure security and resilience planning and preparedness, exercises and training, public awareness, and associated implementation activities and requirements • Identifying, developing, and sharing information within the sector (both public and private sector members) concerning effective cybersecurity practices, such as cybersecurity working groups, risk assessments, strategies, and plans • Providing input to the government on the sector's research and development efforts and requirements
Contact Your SCC to:	Gain knowledge of industry and government actions on critical infrastructure protection priorities for sector and cross sector issues.
How to Connect:	The DHS website provides more information on each of the 16 critical infrastructure sectors, including SCC charters and membership: https://www.dhs.gov/scc
SCCs in Action:	See the Havex/BlackEnergy use case in Section 4.1 on page 45 and the Metcalf substation use case in Section 4.2 on page 50.
SCC Websites:	• Chemical (CSCC): www.chemicalcybersecurity.org • Commercial Facilities: https://www.dhs.gov/commercial-facilities-sector-council-charters-and-membership • Communications (CSCC): www.commscc.org • Critical Manufacturing (CMSCC): https://www.dhs.gov/critical-manufacturing-sector-council-charters-membership • Dams (DSCC): https://www.dhs.gov/dams-sector-council-charters-and-membership • Defense Industrial Base (DIBSSC): https://www.dhs.gov/defense-industrial-base-sector-council-charters-and-membership • Emergency Services (ESSCC): www.sheriffs.org/content/emergency-service-sector-coordinating-council-esscc

Sector Coordinating Councils (SCCs)

- Energy
  - Electricity Subsector (ESCC): http://www.electricitysubsector.org/
  - Oil and Natural Gas Subsector (ONGSCC): https://www.dhs.gov/energy-ong-subsector-charters-and-membership
- Financial Services (FSSCC): www.fsscc.org
- Food and Agriculture (FASCC): https://www.dhs.gov/food-and-agriculture-sector-council-charters-and-membership
- Government Facilities (GFSCC): https://www.dhs.gov/government-facilities-sector-council-charter-membership
- Healthcare and Public Health (HSCC): www.phe.gov/cip
- Information Technology (ITSCC): www.it-scc.org
- Nuclear Reactors, Materials, and Waste (NRMWSCC): https://www.dhs.gov/nuclear-sector-council-charters-and-membership
- Transportation (TSCC): https://www.dhs.gov/transportation-sector-charters-and-membership
- Water and Wastewater Systems (WSCC): https://www.dhs.gov/water-sector-council-charters-and-membership

Sector-Specific Agencies (SSAs)	
Category:	Entities with Critical Infrastructure Security and Resilience Program, Policy, and Mitigation Responsibilities (See Appendix C)
General Description:	Presidential Policy Directive 21 (PPD-21), *Critical Infrastructure Security and Resilience*, advances a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure. Each critical infrastructure sector has unique characteristics, operating models, and risk profiles. As a result, PPD-21 designates a Sector-Specific Agency (SSA) or co-SSAs for each sector that has institutional knowledge and specialized expertise about its sector(s). For sectors subject to Federal or State regulation, the SSA collaborates with the regulator, as appropriate. SSAs promote sector-wide information sharing and support the national program by addressing joint national priorities and reporting on progress toward achieving security and resilience outcomes.
SSA Roles and Responsibilities Related to Critical Infrastructure Owners/Operators and the Private Sector:	Each SSA employs its particular knowledge and expertise to: • Coordinate and collaborate with DHS and other relevant Federal departments and agencies, with critical infrastructure owners and operators, with independent regulatory agencies (where appropriate), and with SLTT entities, as appropriate, to implement PPD-21 • Serve as a day-to-day Federal interface for the dynamic prioritization, collaboration, and coordination of sector-specific activities • Carry out incident management responsibilities consistent with statutory authority and other appropriate policies, directives, or regulations • Provide, support, or facilitate technical assistance and consultations for that sector to identify vulnerabilities and help mitigate incidents, as appropriate • Support the Secretary of Homeland Security's statutory reporting requirements by providing, on an annual basis, sector-specific critical infrastructure information
Contact Your SSA to:	Each SSA varies, but you should contact each SSA (contact information on the following pages) to see if they can help you to: • Coordinate and collaborate with sector-specific government and industry partners to develop collaborative strategies that advance critical infrastructure security and resilience • Identify needs and gaps in planning, initiatives, policies, and procedures that impact the sector's critical infrastructure protective posture • Share information pertaining to threats, vulnerabilities, security, and response and recovery activities that affect sector and cross-sector operations • Receive access to sector-specific handbooks, guides, and web-based training courses
How to Connect:	• See below for a list of the SSAs and their associated sectors • See below for websites and contact information for the various SSAs • The DHS website provides more information on each of the 16 critical infrastructure sectors, including Sector-Specific Plans: https://www.dhs.gov/sector-specific-agencies
SSAs in Action:	DHS, as the SSA for Commercial Facilities, sponsors the Classified Intelligence Forum for the Private Sector (CIF). Within DHS, the Office of Intelligence and Analysis (I&A) and the National Protection and Programs Directorate (NPPD) host bimonthly meetings at DHS Headquarters with appropriately cleared private sector critical infrastructure representatives within the Commercial Facilities Sector and the Cross Sector Coordinating Council (CSCC). The CIF has been expanded regionally to solicit feedback from private sector representatives. That feedback can help to inform the development of current and future intelligence products and other appropriate information sharing or analytic initiatives.

Sector-Specific Agencies (SSAs)

SSAs and Critical Infrastructure Sectors:	Sector-Specific Agency	Critical Infrastructure Sector
Source: PPD-21, Critical Infrastructure Security and Resilience, February 12, 2013: https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil, and Appendix B of the NIPP 2013 (p. 43): http://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience	Department of Agriculture (USDA)[56] Food and Drug Administration (FDA)[57]	Food and Agriculture
	Department of Defense (DOD)	Defense Industrial Base
	Department of Energy (DOE)	Energy[58]
	Department of Health and Human Services (HHS)	Healthcare and Public Health
	Department of the Treasury	Financial Services
	Environmental Protection Agency (EPA)	Water and Wastewater Services
	Department of Homeland Security (DHS)	Chemical Commercial Facilities Communications Critical Manufacturing Dams Emergency Services Information Technology Nuclear Reactors, Materials, and Waste
	Department of Homeland Security General Services Administration (GSA)	Government Facilities[59]
	Department of Homeland Security Department of Transportation (DOT)	Transportation Systems

SSA Points of Contact:[60]

Sector	Agency/ Organization	Office/Center	Email	Website
Chemical	DHS	Office of Infrastructure Protection	chemicalsector@hq.dhs.gov	www.dhs.gov/chemical-sector
Critical Manufacturing			criticalmanufacturing@hq.dhs.gov	www.dhs.gov/critical-manufacturing-sector
Commercial Facilities			cfsteam@hq.dhs.gov	www.dhs.gov/commercial-facilities-sector
Dams			dams@hq.dhs.gov	www.dhs.gov/dams-sector
Emergency Services			ESSTeam@hq.dhs.gov	www.dhs.gov/emergency-services-sector

[56] The Department of Agriculture is responsible for agriculture and food (meat, poultry, and processed egg products).

[57] The Food and Drug Administration is responsible for food other than meat, poultry, and processed egg products.

[58] The Energy Sector includes the generation, refining, storage, transmission, and distribution of oil, gas, and electric power while the Department of Homeland Security is the SSA for commercial nuclear power facilities and for dams.

[59] The Department of Education is the SSA for the Education Facilities Subsector of the Government Facilities Sector; the Department of the Interior is the SSA for the National Monuments and Icons Subsector of the Government Facilities Sector.

[60] Selected from Critical Infrastructure Security and Resilience Functional Relationships – DHS, June 2013; updated April 2016.

Sector	Agency/ Organization	Office/Center	Email	Website
Nuclear Reactors, Materials, and Waste			NuclearSSA@hq.dhs.gov	www.dhs.gov/nuclear-reactors-materials-and-waste-sector
Communications		Office of Cybersecurity and Communications (CS&C)	Comms_Sector@hq.dhs.gov	www.dhs.gov/office-cybersecurity-and-communications
Information Technology			—	www.dhs.gov/office-cybersecurity-and-communications
Transportation Systems		Transportation Security Administration (TSA)	TransportationSector@tsa.dhs.gov	http://www.dhs.gov/transportation-systems-sector
		United States Coast Guard – Office of Port and Facility Compliance	—	www.uscg.mil/hq/cg5/cg544
	DOT	Office of the Secretary	—	www.transportation.gov/mission/administrations/intelligence-security-emergency-response/security-policy-plans-division
Government Facilities	DHS	Federal Protective Service	NIPP-GFS@hq.dhs.gov	www.dhs.gov/government-facilities-sector
	GSA		—	
Defense Industrial Base	DOD	Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs	RSS.DCIPOffice@osd.mil	http://policy.defense.gov/OUSDPOffices/ASDforHomelandDefenseGlobalSecurity/DefenseCriticalInfrastructureProgram/Roles.aspx
Energy	DOE	Office of Electricity Delivery and Energy Reliability – Infrastructure Security and Energy Restoration Division	doehqeoc@oem.doe.gov	http://energy.gov/oe/mission/infrastructure-security-and-energy-restoration-iser
Financial Services	Treasury	Office of Critical Infrastructure Protection and Compliance Policy	OCIP@treasury.gov	www.treasury.gov/about/organizational-structure/offices/Pages/--Office-of-Critical-Infrastructure-Protection-and-Compliance-Policy.aspx
Food and Agriculture	USDA	Office of Homeland Security and Emergency Coordination	nsps@dm.udsa.gov	www.dm.usda.gov/ohsec/hsd/fas.html
	FDA	Office of Food Defense, Communication, and Emergency Response	fooddefense@fda.hhs.gov	www.fda.gov/Food/FoodDefense/default.htm
Healthcare and Public Health	HHS	Office of the Assistant Secretary for Preparedness and Response	cip@hhs.gov	www.phe.gov/Preparedness/planning/cip/Pages/default.aspx
Water and Wastewater Systems	EPA	Water Security Division	—	www.epa.gov/waterresilience

United States Coast Guard (USCG) – Area Maritime Security Committees (AMSC) and Waves on the Waterfront (WOW)	
Category:	Partnerships, Alliances, and Councils – Sector-Specific
General Description:	**Area Maritime Security Committees (AMSCs)** are public-private partnerships throughout the country that coordinate with the USCG to address local issues relating to the security and protection of a port or waterway. Membership is typically comprised of local representatives from government agencies, maritime labor and industry organizations, and public interest groups. AMSCs exist in each Captain of the Port (COTP) zone and are the cornerstones of security in the Nation's ports. **Waves on the Waterfront (WOW)** is a bimonthly periodical developed by the Coast Guard's Office of Port and Facility Compliance to keep stakeholders abreast of safety, security, and stewardship concerns.
Functions, Products, and Services Relevant to the Critical Infrastructure Community:	**AMSCs:** • Serve as a link between port stakeholders to communicate threats and changes in Maritime Security Levels and disseminate appropriate security information • Identify critical port infrastructure and operations • Identify risks, threats, vulnerabilities, and consequences • Determine mitigation strategies and implementation methods • Develop and describe the process for continually evaluating overall port security through consideration of consequences and vulnerabilities, how they may change over time, and what additional mitigation strategies can be applied • Provide advice to and assist the COTP in developing the Area Maritime Security Plan (AMSP) • Ensure that a risk-based Area Maritime Security Assessment is completed by the AMSC itself, the local COTP, a Coast Guard Port Security Assessment team, or by a third party **WOW:** • Release a bimonthly newsletter
Contact AMSC or WOW to:	• To get more information on AMSCs • To be added to the WOW distribution list • To submit articles for consideration in WOW
How to Connect:	• AMSC website with brochure link: http://www.uscg.mil/hq/cg5/cg544/amsc.asp • AMSC email: AMSC@uscg.mil • WOW and AMSC POC: CG-FAC@uscg.mil
AMSCs in Action:	Threat information through the USCG COTP's on a case by case basis through the AMSC.
WOW in Action:	Recent issues can be found at: http://www.uscg.mil/hq/cg5/cg544/Waves%20on%20the%20Waterfront.asp

Page intentionally left blank.

SECTION 4.0

Use Cases

The following use cases illustrate how threat information was shared in four real situations addressing a variety of threats:

1. Cyber: Havex and BlackEnergy (2014)
2. Physical: Metcalf Incident (2013)
3. International: Westgate Mall Attack in Kenya (2013)
4. National Special Security Event: 2013 Presidential Inauguration

In addition to the graphic in each use case, see Appendix G for a more detailed visualization of the information flows in each of the use cases.

4.1 Cyber Use Case: Havex and BlackEnergy (2014)

This use case illustrates the engagement between private cybersecurity firms, industrial control firms, and Federal outreach and engagement stakeholders in response to two cyber threats. Note that this is not a comprehensive explanation of all information sharing involved with this case. Inputs were limited by responses to requests for information.

4.1.1 Background

This cyber use case addresses a pair of malware threats to industrial control systems (ICS) that were first identified in mid-2014, but began in early 2011. The first, called Havex, was brought to the attention of the National Cybersecurity and Communications Integration Center (NCCIC) by private sector cybersecurity firms. The second piece of malware, called BlackEnergy, was discovered by trusted third-party partners. Since both cyber threats had aspects that targeted the ICS systems of U.S. critical infrastructure, the DHS ICS Cyber Emergency Response Team (ICS-CERT), which is part of the NCCIC, took the lead in conducting coordinated outreach, mitigation, and response on behalf of the Federal Government.

The Havex malware was used for a variety of purposes; however, there was an ICS-focused variant leveraged in a campaign that used multiple vectors for infection. The vectors employed included phishing emails, webpage redirects, and infected ICS software installers. The most successful vector of infection was the software installers on the ICS vendors' websites. When unsuspecting ICS operators downloaded an updated version of ICS software, they unwittingly installed the Havex malware on their machines as well. Based on reporting from researchers at two private sector computer security vendors and subsequent analysis by the NCCIC, the malware demonstrated capabilities to scan and access control system environments, including potentially manipulating the process. The Havex threat actor demonstrated familiarity with a control system specific technology (Open Platform Communications or OPC protocol) and was able to use that capability to scan and interrogate the compromised network for control system devices. Development of this capability also indicates the threat actor conducted some level of research and testing to develop the Havex malware.

The BlackEnergy malware exploited previously unknown vulnerabilities in the human-machine interface (HMI), where the operator monitors and operates the control system, of at least three ICS vendor products. With access to an HMI, an intruder can do anything the legitimate operator can do, such as turn equipment on or off, see the status of the process, and change the set points of the system, including the allowable level of a tank or the maximum temperature setting. The depth of these potential intrusions into a control system poses a serious threat to the stability of the process and creates the potential for physical consequences. Analysis of the BlackEnergy threat actor's techniques revealed a focused effort to find and exploit previously unknown vulnerabilities in control system devices and software. This effort required specific research into control system devices and software along with testing to gain the capability to launch a successful attack.

These two campaigns illustrate the concerted efforts by sophisticated actors for at least four years to understand critical infrastructure control systems, discover unknown/unpatched vulnerabilities for exploitation, and to use "out-of-the-box" techniques for gaining access to the operational environment. While the full scope of penetration into ICS systems remains unknown, the coordinated outreach campaign launched by the Federal Government in response to these threats has informed and educated many companies and entities, and has potentially affected individuals who have responsibility for ICS.

4.1.2 Threat Information Sharing

4.1.2.1 DHS – NCCIC

The NCCIC and its component, ICS-CERT, worked in concert with the FBI to identify potential threat actors and to perform traditional incident response activities. An in-depth 47-page analytic report on Havex and BlackEnergy was created and distributed via For Official Use Only (FOUO) channels with a two-page summary for executives. The NCCIC also conducted other threat information-sharing activities:

- Coordinated with affected vendors to identify software vulnerabilities and get them patched
- Developed a custom detection algorithm and distributed it on the public website
- Released a series of Unclassified//For Official Use Only (U//FOUO) level alerts to the critical infrastructure community through the ICS portal, the Homeland Security Information Network (HSIN) portal, and the ICS-CERT public website, while also working with intelligence and law enforcement to limit the amount of information that could be leveraged by adversaries
- Conducted an "Action Campaign" consisting of "Secret" briefings in 13 cities to over 1700 cleared stakeholders and coordinated outreach for the Campaign through Information Sharing and Analysis Centers (ISACs); Sector-Specific Agencies (SSAs); State, local, tribal, and territorial (SLTT) partners; DHS Office of Infrastructure Protection's (IP) Protective Security Advisors (PSAs); fusion centers; and the FBI
- Conducted "Secret" level Secure Video Teleconference (SVTC) with fusion centers and FBI field offices
- Provided briefings at all normal ICS-CERT outreach activities (weekly, monthly, quarterly, ad-hoc) at "Unclassified" and "Secret"

- Worked with the Intelligence Community (IC) to better understand and describe the threat

4.1.2.2 Multi-State ISAC (MS-ISAC)

The Multi-State ISAC (MS-ISAC) helped share information by disseminating a presentation by ICS-CERT on the Cyber Risks to Industrial Control Systems, titled "BlackEnergy & Havex Briefing for Partners" in April 2015. The MS-ISAC also deployed signatures to detect Havex and Black Energy in Albert,[61] but this has not had any confirmed hits.

4.1.2.3 U.S. Department of Energy (DOE)

DOE received intelligence message traffic about BlackEnergy and Havex cases from private sector cybersecurity vendors. DOE conducted a manual check and was able to verify that none of their companies were on one of the vendor's or ICS-CERT's lists. DOE worked through ISACs to share unclassified information and open source information with members. They requested that the ISACs share the information with their members as a Request for Information (RFI). As a result, owners and operators were able to share any information which they had pertaining to the BlackEnergy/Havex cases with the ISACs. ISAC members with clearances and customers with limited clearances were briefed in-person at DOE offices and received information up to the Top Secret/Sensitive Compartmented Information (TS/SCI) level. DHS held a regional Havex/BlackEnergy campaign and DOE encouraged owners/operations to attend the regional meetings, which shared information at the "Secret" level.

4.1.2.4 DHS – IP

When needed (as in the Havex and BlackEnergy cases), IP elevates its outreach by convening a special topic engagement working group to bring together potentially affected private sector partners and representatives from the Federal Government to discuss a specific threat or issue. These working groups are created to augment IP's typical role of facilitating government and private sector collaboration and coordination through the Critical Infrastructure Partnership Advisory Council (CIPAC) process.

During the Havex and BlackEnergy cases, the unclassified special topic engagement working group reached out to Sector Coordinating Council (SCC) leaders, subject matter experts, and other high-level representatives to convene a meeting to share threat information. Approximately 30 private sector representatives participated in person, and several participated via a conference call line. During the meeting, ICS-CERT gave a briefing on the BlackEnergy/Havex threat, including information on the threat's background and mitigation strategies. Based on consensus advice and recommendations from the attendees following the meeting, ICS-CERT prepared a BlackEnergy/Havex one-pager, targeted at senior executives that summarized the threat and potential consequences and was distributed by IP, including

[61] Albert is the MS-ISAC Netflow/Intrusion Detection System Monitoring and Analysis Service, which provides their partners with a near real-time automated process that identifies and alerts on traditional and advanced threats on a network, facilitating rapid response to threats and attacks. The Albert sensor(s) provide traditional Intrusion Detection System (IDS) monitoring, along with netflow and passive DNS collection and analysis. Through its 24/7 Security Operations Center (SOC), MS-ISAC manages the sensor(s) to identify malicious activity, and, in accordance with escalation procedures prescribed by the partner, provides notification of malicious activity.

being posted to the Homeland Security Information Network (HSIN)[62]. Additionally, a BlackEnergy/Havex tab was created and posted on HSIN to provide a "live" feed of BlackEnergy/Havex information.

4.1.2.5 DHS – Office of Intelligence and Analysis (I&A)

In June 2015, I&A, in collaboration with ICS-CERT, published a Field Analysis Report (FAR)—a finished intelligence analysis product, "(U//FOUO) Recent Malware Campaigns Highlight Threat to Rocky Mountain Region Industrial Control Systems"—that provided an analysis of how the Havex and BlackEnergy malware campaigns impacted critical infrastructure in the Rocky Mountain Region. This analysis was based on evidence and research gathered by ICS-CERT and from technical open source reports from antivirus vendors. The product was published and shared by I&A and its deployed field personnel through multiple mediums, including threat briefings, the HSIN-Intel Community of Interest, informational emails, hand delivery to key customers, and scheduled phone calls. It was primarily disseminated to and consumed by Federal, SLTT, and private sector partners—to include State and major urban area fusion centers—in order to help assess risk and deploy mitigation resources. I&A also published a number of Intelligence Information Reports (IIRs) detailing BlackEnergy malware campaigns against State, local, and private sector facilities in Ohio, North Carolina, Massachusetts, California, Georgia, and Alabama. These reports were made available to the IC and have received positive feedback from multiple community partners.

4.1.2.6 DHS – Transportation Security Administration (TSA)

TSA, as one of the Sector-Specific Agencies (SSAs), worked with ICS-CERT to ensure stakeholder attendance at the regional "Secret" briefings. TSA's Office of Intelligence and Analysis (OIA) also included the facts of the use case in various "Secret" and "Unclassified/Sensitive Security Information (U/SSI)" assessments that were shared with the following stakeholders through the following mechanisms:

- Classified Enclaves "Secret":
  - Email (United States Government (USG) partners)
  - In-person (USG and private sector)
  - Secure Video Teleconference (SVTC) (USG and private sector)
  - Secure teleconference (USG and private sector)
  - Joint Worldwide Intelligence Communication Systems (JWICS) (including National Counterterrorism Center (NCTC) Online) (USG partners)
  - Homeland Secure Data Network (HSDN) (including NCTC Online) (USG partners)
  - Transportation Security Administration Remote Access to Classified MOVI (TRACE MOVI) (USG and private sector)
  - Classified discussions and/or reading of classified materials for those not in the National Capital Region through TSA Field Intelligence Officers
- Unclassified (including FOUO and SSI) for both USG and private sector partners:

[62] HSIN is the trusted network for homeland security mission operators and partners to share Sensitive But Unclassified information. Federal, SLTT, international, and private sector homeland security partners use HSIN to manage operations, analyze data, send alerts and notices, and in general, share the information they need to do their jobs.

- Email
- In-person
- Teleconference
- HSIN

In this use case and all others, when the FBI issues a Joint Threat Assessment (JTA) or DHS sends out a Joint Intelligence Bulletin, Field Analysis Report, or DHS Terrorism Report, TSA's OIA sends the information to its network of Field Intelligence Officers (FIOs). If the information is classified, the Field Intelligence Division's Intelligence Integration Branch (IIB) reviews and submits information via a collateral "Secret" TRACE MOVI version to the FIOs. Regularly, this information also has dissemination instructions on who it is to be shared with in the field, including Federal partners or private stakeholders. Finally, some of the material is also rolled up into a daily classified summary report called the Daily Field Information Report (DFIR)[63] for dissemination to the field.

[63] The DFIR used to be called the Strategic Transportation Threat Awareness Report (STTAR).

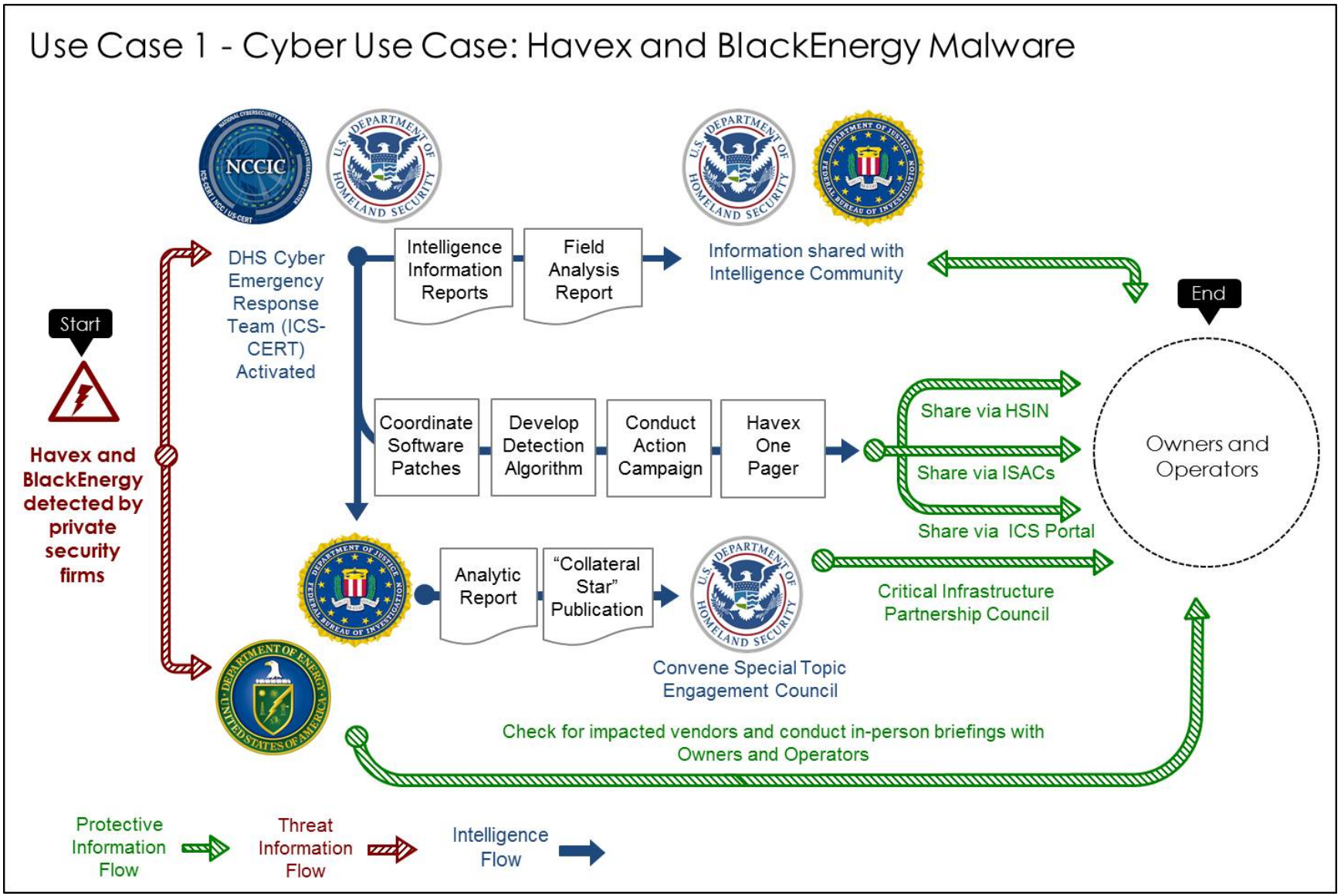


Figure 9: Use Case 1 – Cyber Use Case: Havex and BlackEnergy Malware

4.2 Physical Use Case: Metcalf Electric Substation Incident (2013)

This use case illustrates the threat information sharing that occurred in the aftermath of a physical attack on an electric power substation that included the severing of fiber optic cables. The use case also discusses various methods of national outreach that occurred during the year following the incident. Note that this is not a comprehensive explanation of all information sharing involved with this case. Inputs were limited by responses to requests for information.

4.2.1 Background

On April 16, 2013, attackers fired more than 100 rounds of gunfire into the cooling radiators of 17 electricity transformers at a Pacific Gas and Electric (PG&E) electric substation in Metcalf, CA. The gunfire caused the radiators to leak thousands of gallons of cooling oil. An alarm showing a drop in pressure alerted PG&E personnel to shut down the transformers to prevent permanent damage. Despite the radiator attack, PG&E was able to successfully re-route electric power to avoid any power loss to customers. However, in addition to shooting the transformer radiators, the attackers also severed two groups of fiber optic cables in an area adjacent to the substation. Severing these cables disrupted landline phone service, including 911 service, across a portion of Santa Clara County, CA. The dual attack took about one hour and caused millions of dollars in damage. The individual(s) responsible for the attack have not been identified.

4.2.2 Threat Information Sharing

4.2.2.1 PG&E

Following the attack, PG&E immediately contacted local law enforcement and increased security, providing a 24/7 presence at its Metcalf substation and other significant substations by adding additional guard posts with support from Santa Clara County law enforcement personnel. The Santa Clara County Sheriff's Office led the investigation with the San Jose Police Department. The San Francisco FBI Field Office also opened an investigation.

After contacting local law enforcement, PG&E immediately filed an Electric Emergency Incident and Disturbance Report (Form OE-417) with the Office of Electricity Delivery and Energy Reliability (OE) within the U.S. Department of Energy (DOE), and filed a Suspicious Activity Report (SAR) with the U.S. Department of Homeland Security (DHS) Office of Infrastructure Protection (IP). This initiated circulation of information about the incident to other Federal partners.

Following the attack, PG&E reached out to public and private partners to share incident and threat information through the following steps:

- Via teleconference, the PG&E Dams Sector Coordinating Council (SCC) representative[64] discussed the situation with the chair of the Dams SCC.
- Following that call, PG&E briefed the Dams Sector Joint Council, consisting of the Dams SCC and the Dams Government Coordinating Council (GCC)

[64] PG&E is also a member of the Dams SCC.

- PG&E also briefed the Electricity Subsector Coordinating Council (ESCC) during a call that the Council convened to provide situational awareness, share information, and coordinate members. IP coordinated with the ESCC to bring in members from the Federal Energy Regulatory Commission (FERC), Federal Communications Commission (FCC), Department of Energy (DOE), FBI, and the Northern California Regional Intelligence Center (NCRIC) to participate.
- PG&E also briefed the Edison Electric Institute (EEI) to provide situational awareness and share relevant information.

As new information became available, the PG&E security director continued to share with partners and present updated briefings to the SCCs, EEI, and the DOE. Other private sector energy providers received information through SAR reports and the Homeland Security Information Network – Critical Infrastructure (HSIN-CI) and HSIN-Dams web portals.

In addition to sharing information, PG&E provided IP's Protective Security Advisors (PSAs) in California with access to its major substations to conduct security surveys that supported threat mitigation. Since the incident, the local PSAs have been providing continuing assistance to PG&E with security vulnerability assessments, protective measure option development, and security planning. As a result of the attack, many energy owners/operators also conducted a review of their critical assets and current security measures. Subsequently, they developed plans to address gaps and vulnerabilities and implemented additional measures to be prepared for similar attacks in the future. For example, based on the Metcalf event, Dominion (providing electricity to Virginia and North Carolina) developed a seven-year, $500 million security enhancement plan, known as the "Dominion Reliability and Security Program."

4.2.2.2 Department of Energy (DOE)

As the Sector-Specific Agency (SSA) for the Energy Sector, DOE conducted an information and coordination call with representatives from DHS, FERC, FCC, FBI, and NCRIC.

4.2.2.3 DHS – IP

IP also hosted a separate situational awareness call with FERC, FCC, FBI, and NCRIC. Initial actions were followed by engagements with public and private sector stakeholders within the Energy Sector in which stakeholders discussed the relevance of the incident, and information sharing efforts were expanded to related critical infrastructure sectors, such as the Dams Sector. All related Situational Awareness Reports (SARs) were forwarded through the National Infrastructure Coordinating Center (NICC) to associated Energy Sector critical infrastructure stakeholders and PSAs.

4.2.2.4 NCRIC, NERC, and ES-ISAC

Alerts were sent out by NCRIC, the North American Electric Reliability Corporation (NERC), and the Energy Sector ISAC (ES-ISAC) to their sector partners, including critical infrastructure owners and operators, without specifically mentioning PG&E.

4.2.2.5 California Joint Regional Intelligence Center (JRIC)

Three months after the attack, information sharing evolved into collaborative training. On July 23, 2013, the California Joint Regional Intelligence Center (JRIC) sponsored a training event to discuss the incident and share lessons learned. Speakers included representatives from PG&E Security and another California energy firm. PSAs in California also attended the briefing.

4.2.2.6 Collaborative Initiative

Additionally, in response to the Metcalf incident, DHS and DOE, in coordination with interagency and private sector partners, initiated an outreach campaign to raise security awareness across the Electricity Subsector. The Electric Substation Security Awareness Campaign kicked off in December 2013 and concluded in March 2014. It was conducted in collaboration with ESCC, ES-ISAC, FBI, FERC, and multiple industry partners, including PG&E. This “road show” took place in 10 U.S. cities and 3 Canadian cities. Each event included a series of briefings, along with a panel discussion, to raise awareness on the evolving risk environment and promoted increased collaboration on risk mitigation strategies, protective measures and industry best practices. The sessions were initially open to stakeholders from the electricity owner and operator community and law enforcement entities, but were expanded to incorporate stakeholders from the Emergency Services, Oil and Natural Gas, and Nuclear Sectors.

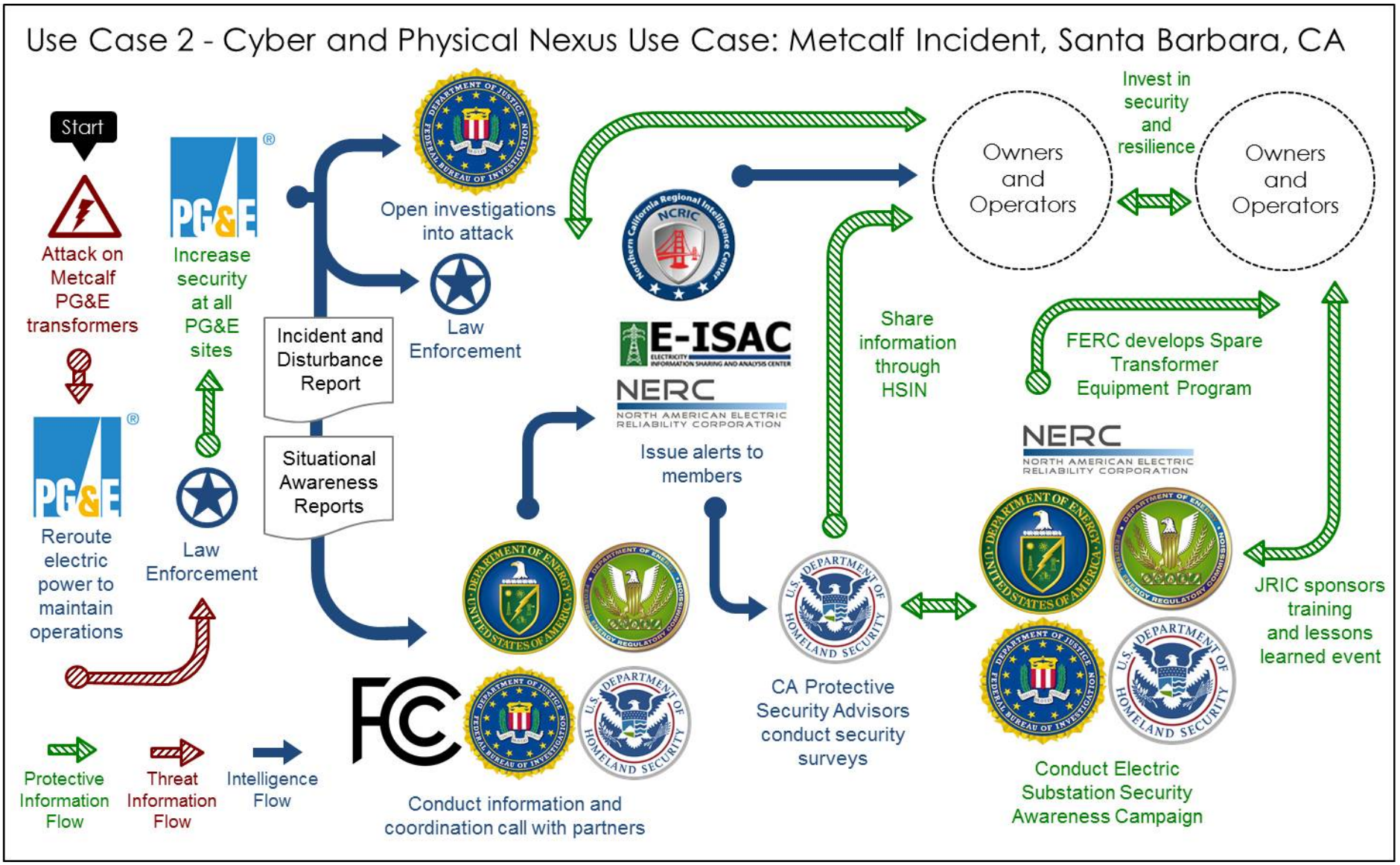


Figure 10: Use Case 2 – Cyber and Physical Nexus Use Case: Metcalf Incident, Santa Barbara, CA

4.3 International Use Case: Westgate Mall Attack in Nairobi, Kenya (2013)

The 2013 Westgate Mall attack in Nairobi, Kenya, was of high interest to the U.S. private sector as it demonstrated the vulnerability of the open access model used in most commercial facilities, including U.S. shopping centers. The tactics, techniques, and procedures used were important for stakeholders to understand in order to drive preparations. This use case illustrates the Federal outreach and engagement with Commercial Facilities Sector partners following the Westgate Mall attack. Note that this is not a comprehensive explanation of all information sharing involved with this case. Inputs were limited by responses to requests for information.

4.3.1 Background

On September 21, 2013, four attackers stormed the Westgate Shopping Mall in Nairobi, Kenya, armed with guns and grenades. The attackers mounted an assault that culminated in a four-day stand-off with Kenyan security forces. The Somali group Al-Shabaab claimed responsibility for the attack, making it the group's largest attack since a pair of coordinated suicide bombings in Uganda that killed 70 people in 2010. The group asserted that the Westgate attack was intended to retaliate against the Kenyan government for its involvement in the Somali conflict.

All told, the clash left at least 71 people dead (including six security officers and all four gunmen) and more than 175 injured. Additionally, the Kenyan government stated it rescued over 1,000 individuals. A number of U.S. companies owned storefronts at Westgate, and several U.S. companies had employees in the shopping center at the time of the attack. A temporary duty employee of Ball Corporation was shot during the incident and subsequently received a medical evacuation back to the United States.

4.3.2 Threat Information Sharing

4.3.2.1 U.S. State Department Overseas Security Advisory Council (OSAC)

The State Department's Overseas Security Advisory Council (OSAC), which promotes open dialogue on security issues between the U.S. Government and the American private sector abroad, contributed to the initial U.S. Government response to the Westgate attack, coordinating both short- and long-term information sharing and response efforts related to the incident. The OSAC Country Council in Nairobi quickly began to exchange information about the attack by using web-based applications to post closed-circuit television (CCTV) footage shared by one of OSAC's private sector members, and to provide on-scene updates. This information enabled the U.S. State Department Diplomatic Security's Regional Security Officer to further coordinate with the appropriate FBI Legal Attaché, as well as with other Federal offices involved in the response. OSAC's East Africa regional analyst also flew to Nairobi the week following the attack to chair the Country Council meeting. Following OSAC's participation in a DHS-sponsored conference call related to the incident, over 50 OSAC constituents (including commercial facilities and transportation owners and operators) contacted OSAC to request consultations with their regional analysts.

In general, OSAC's regional analysts provide one-on-one consultations on an ad hoc basis with registered constituent representatives to provide expert security advice or analysis regarding a range of regional concerns. Consultations can be widely varied: some are intended to provide a

general situational awareness about a given environment, while others are more focused on a specific security concern.

4.3.2.2 Real Estate ISAC (RE-ISAC)

Upon notification of the attack, the Real Estate Information Sharing and Analysis Center (RE-ISAC) began communicating with members regarding the incident. It shared a brief summary one day after the incident with members and also distributed that summary to public sector partners for awareness, including DHS-Office of Infrastructure Protection (IP) (including IP's Protective Security Advisors (PSAs)); DHS Office of Intelligence and Analysis (I&A); the Domestic Security Alliance Council (DSAC); OSAC; FBI; and fusion centers. It provided updates via routine daily reports that utilized open source research platforms, intelligence providers (from various subscriptions), and government updates and analysis (including information shared by DHS and OSAC). Over the following days the RE-ISAC continued to share updates from OSAC with their members, including providing updates on some of the cascading impacts the incident had on domestic facilities. In the weeks that followed, senior RE-ISAC leadership provided situational updates by phone and email to the cross-sector community (such as on the October 2013 National Council of ISACs call), to sector and subsector colleagues (as members began preparations for the holiday shopping season), and with Federal government partners at all levels (primarily FBI and DHS), fusion centers, and law enforcement as members worked with the government to conduct holiday season preparedness exercises.

RE-ISAC and members continue to monitor events closely and were very engaged when Al-Shabaab released their February 2015 videos threatening Western malls. At that time, RE-ISAC helped provide awareness of the threat to members, partners, and other sector ISACs.

4.3.2.3 Federal Bureau of Investigation (FBI)

Following the initial Westgate attack, FBI field offices provided threat briefings to Joint Terrorism Task Force (JTTF) partners, including the JTTF Executive Boards, Military Working Groups, private sector owners and operators, mall security organizations, and law enforcement personnel. The information provided in these briefings ranged from breaking news reports to initial investigative findings and other forms of raw intelligence (tailored at the appropriate classification level for each audience). The FBI also shared threat information through email and the InfraGard portal, and many FBI field offices held video teleconferences to discuss lessons learned from Westgate.

The FBI also worked with DHS and other partners to provide more intensive, longer-term efforts to train and educate owners and operators of U.S. malls and retailers on best practices related to complex attacks. Following the incident, the FBI asked the Sector Outreach and Programs Division (SOPD), in DHS-IP, to quickly make key industry connections, and SOPD, in turn, contacted the Commercial Facilities Sector Coordinating Council (SCC) to recruit key leaders in the Shopping Center Subsector Council. Those leaders then communicated the importance of this initiative to their networks and encouraged their active participation. Together, the FBI and IP facilitated 56 discussions at FBI field offices across the country from December 6-9, 2013. Participants included State, local, private sector, and Federal partners (including IP's PSAs). FBI field offices also conducted 61 table top exercises, 57 command post exercises, and 53 full-scale exercises to test preparedness plans and procedures for a scenario similar to the Westgate attack. In total, there were 9,472 participants.

4.3.2.4 The Joint Counterterrorism Assessment Team (JCAT)

The JCAT, a joint team with Federal and SLTT first responders (led by the National Counterterrorism Center (NCTC), with FBI and DHS deputies) produced "*Complex Operating Environment for First Responders During Emergency Responses – Shopping Malls"* on December 20, 2013, to assist with emergency response for shopping malls. This product was also shared with the private sector through InfraGard and DSAC, and was posted on the FBI's Law Enforcement Enterprise Portal (LEEP) and Homeland Security Information Network (HSIN).

4.3.2.5 DHS – Federal Emergency Management Agency (FEMA)

Exercises and workshops, organized by the NCTC, FBI, and FEMA, have been ongoing since the 2008 Mumbai attack. For example, the Joint Counterterrorism Awareness Workshop Series (JCTAWS) is a two-day workshop targeting tier one cities (the U.S's largest cities) designed to improve the ability of local jurisdictions to prepare for, protect against, and respond to complex terrorist attacks. In 2012, FEMA expanded its complex attack portfolio to include a four-day Integrated Emergency Management Course (IEMC), "Preparing Communities for a Complex Coordinated Attack," that focuses on targeting second and third tier cities. Like the workshop, the course is a training initiative designed to strengthen the ability of local jurisdictions to protect against and respond to a complex coordinated attack. Both programs feature briefings (including a threat briefing from the National Counterterrorism Center), case studies, and facilitated discussions based on a community specific attack scenario.[65] Through these scenario-based discussions, participants self-identify gaps in their current operational plans and capabilities, as well as possible solutions.

Following the attacks against Westgate Mall, many communities requested that a mall be included in the JCTAWS and IEMC scenarios. As a result, these communities had robust discussions about how to launch an integrated, coordinated response to an active shooter or complex attack at their malls and key retail sites. Security leadership from the malls participated in the workshops, and the discussions resulted in clearly articulated gaps in planning, coordination, and operational capability that these communities are now addressing moving forward.

4.3.2.6 DHS – IP

Since the Westgate attack, the training approach has evolved in response to changes in the threat environment. In the second half of 2014, violent extremist literature included many calls for attacks on Federal and military installations and commercial facilities, as well as attacks using guns and other weapons of convenience. In October 2014, IP convened an Engagement Working Group (EWG) comprised of retailers, hoteliers, government, and others to discuss the threat situation and the path forward. As a result, IP, the Interagency Security Committee (ISC),[66] and the NCTC embarked on the Enhanced Security Outreach Initiative, an 11 city campaign that featured threat briefings and open forum discussions. The Initiative brought

[65] Private sector partners involved with both the JCTAWS and IEMC typically include telecommunications/network providers; utilities; major employers—insurance, financial, manufacturing, chemical, logistics, and tourism; hotels; special event venues; downtown business district/chamber representatives; and non-profit organizations—American Red Cross, Volunteer Organizations Active in Disasters (VOAD), or faith-based networks. Since 2010, 20 JCTAWS workshops have been conducted with more than 4,500 participants.

[66] The ISC's mandate is to enhance the quality and effectiveness of physical security in, and the protection of buildings and nonmilitary Federal facilities in the United States.

Federal and commercial partners and emergency responders together in key markets across the country.

After a February 2015 Al-Shabaab video called for further attacks, specifically citing the Mall of America, PSAs completed a surge of mall Infrastructure Survey Tool (IST) assessments.[67] In March 2015, IP convened a similar EWG of private sector partners to discuss how to modify the DHS Active Shooter Preparedness Workshop Series to introduce more adult-education learning techniques and allow for more dynamic exchanges of information with the audience. Finally, IP recently convened another group similar to an EWG—this time including the Department of Defense—following the July 16, 2015, attack on military recruiting and reserve centers in Chattanooga, TN, that resulted in the death of four Marines and one Navy officer. Such working groups examine evolving threats and discuss new approaches to prevent, protect against, and respond to potential attacks.

4.3.2.7 DHS – Office of Intelligence and Analysis (I&A)

I&A also coordinated threat briefings for malls across the country through its Field Operations Division. In Ohio, the I&A Intelligence Officer (IO), in coordination with the local PSA, presented a threat briefing and participated in a roundtable question and answer session at the local fusion center, the Strategic Analysis and Information Center (SAIC). Over 40 security managers from local area malls attended the briefing at the SAIC-organized Local Area Mall Security Meeting at the Ohio Department of Public Safety. In addition, the IO provided a classified threat briefing during the DHS-SAIC Monthly Intelligence and Information Sharing Threat Briefing. The Ohio-based IO also worked with the SAIC to publish a For Official Use Only (FOUO) threat assessment provided specifically to first responders, law enforcement, fire, etc. and released on HSIN-Intel and Ohio's Contact Information Management System (CIMS).

At the Westgate Mall in Kentucky, the KY-deployed IO briefed the threat to local officials during a meeting organized by the local PSA. The IO also briefed other State, local, tribal, and territorial (SLTT) partners, particularly those that may respond or partner with the mall owner operators in a similar case.

Earlier in 2015, I&A and the FBI produced a Joint Intelligence Bulletin (JIB) regarding another threat to malls in late January/early February. The JIB was disseminated to Federal and SLTT partners, as well as to key owners, operators, and private sector partners. Accompanying the JIB to areas of responsibility (AOR) partners, I&A's East Central Region Field Personnel also drafted a cover note—or "View from the Field"—providing regional, State, and local context. The local PSA was able to help disseminate this JIB and cover sheet. This effort also resulted in a suspicious activity report (SAR).

Furthermore, I&A Field Operations South Central Region field personnel also delivered a threat briefing to the Garland Police Department and surrounding law enforcement jurisdictions. This briefing covered the tactics, techniques, and procedures (TTPs) used in the 2013 attack at the Westgate Mall in Kenya, among other international terrorist attacks.

[67] A web-based vulnerability assessment tool that applies weighted scores to identify vulnerabilities and trends for specific infrastructure and across the sector.

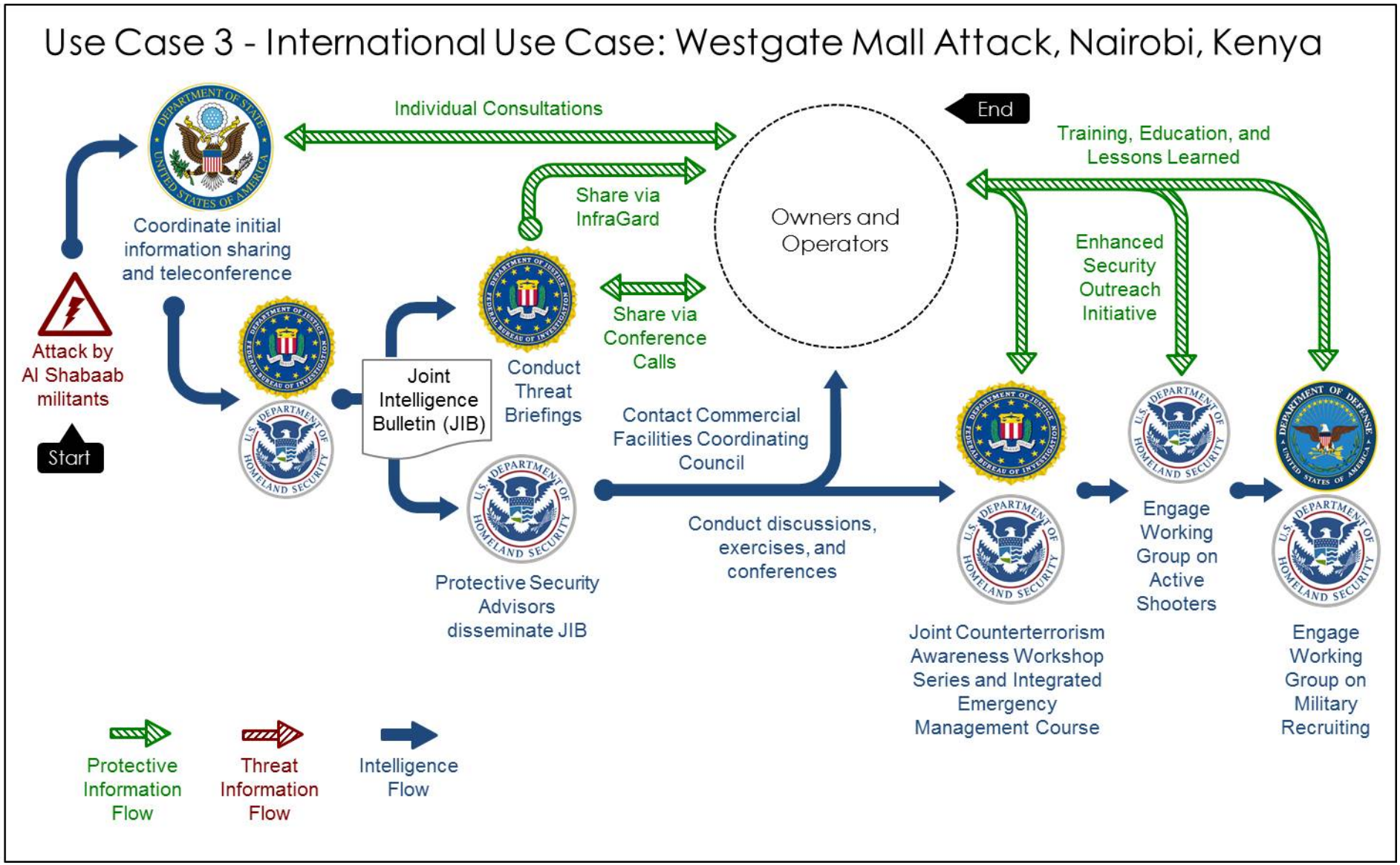


Figure 11: Use Case 3 – International Use Case: Westgate Mall Attack, Nairobi, Kenya

4.4 National Special Security Event (NSSE) Use Case: 2013 Presidential Inauguration

This use case illustrates the structure of engagement between Federal, SLTT, and critical infrastructure owners and operators before and during a pre-planned National Special Security Event (NSSE) requiring heightened cyber and physical security due to large numbers of attendees. Note that this is not a comprehensive explanation of all information sharing involved with this case. Inputs were limited to responses by requests for information.

4.4.1 Background

The Secretary of the Department of Homeland Security (DHS) designated the January 2013 Presidential Inauguration in Washington, D.C., as a NSSE. (An NSSE is an event of national or international significance deemed by DHS to be a potential target for terrorism or other criminal activity. Examples include summits of world leaders, international organization meetings, and presidential nominating conventions.) NSSE designation requires Federal agencies provide full cooperation and support to ensure the safety and security of those participating in or attending the event, as well as the safety and security of the community where the event takes place.

The 2013 Inauguration lasted from January 20–22 and included a variety of public and private events, including the ceremony itself, the accompanying parade, a luncheon, and three official Inaugural Balls. The festivities attracted more than one million attendees to the National Capital Region (NCR), and over 3,000 police officers and military contingents helped ensure the required level of security. Multiple entities shared a variety of threat information both leading up to and during the event, helping to maintain security.

4.4.2 Pre-Event Threat Information Sharing Activities

The FBI and DHS were the principal Federal departments and agencies who shared threat information with critical infrastructure owners/operators and private sector entities regarding the Inaugural events. As with all NSSE events, the FBI was the lead Federal agency for intelligence and crisis management, DHS-Federal Emergency Management Agency (FEMA) was the lead for consequence management, and the DHS-U.S. Secret Service (USSS) was the lead for the coordination of security planning and implementation, pursuant to the Presidential Threat Protection Act of 2000. Additional agencies and offices were involved with other preparatory and real-time monitoring security components.

A Joint Threat Assessment (JTA) was developed and published at the Unclassified//For Official Use Only (U//FOUO) level for the Inaugural events. The JTA addressed international and domestic terrorist, criminal, cyber, and transportation related threats to the Inauguration and the NCR. Members of the intelligence community produce JTAs, and, for NSSEs, the FBI is the lead intelligence organization for their development. Other major contributors included the DHS Office of Intelligence and Analysis (I&A), Joint Forces Headquarters, and the DC Fusion Center—the Washington Regional Threat and Analysis Center. Additional contributing information was provided by the Transportation Security Administration (TSA), the United States Coast Guard (USCG), the National Counterterrorism Center (NCTC), U.S. Capitol Police, the Northern Virginia Regional Intelligence Center, and the Terrorist Screening Center. Once produced, the JTA was shared with Federal, State, and local government agencies and authorities to help them develop and prioritize protective and support measures. It was then widely shared with NCR critical infrastructure owners/operators through HSIN, meetings with

local law enforcement and fusion centers, and unclassified and classified briefings. Other updates were provided as needed. The JTA found no information indicating a credible threat to the 2013 Presidential Inauguration, but it included an assessment of the ongoing threat environment.

4.4.2.1 DHS – United States Secret Service (USSS) and Office of Infrastructure Protection (IP)

In addition to the distribution of the JTA, briefings were provided to Chief Executive Officers (CEOs) by the Critical Infrastructure Protection Sub-Committee (CIPSC), which was led by the USSS and co-chaired by IP. The CIPSC was one of the 28 inaugural subcommittees set up by the Executive Steering Committee (established by the USSS). The CIPSC included over 100 participants from public and private sector entities, including critical infrastructure owners/operators, IP's Protective Security Advisors (PSAs), FBI, U.S. Park Police, county police, and the DC Department of Transportation. The CIPSC was tasked with developing and implementing a critical infrastructure plan with the purpose of monitoring and safeguarding all infrastructure systems in the affected area in order to ensure a safe environment and support the mitigation of potential risks to public safety. The CIPSC focused on physical and virtual critical infrastructure in the NCR and Mid-Atlantic Region that was so vital that incapacity or destruction of that infrastructure may have had a debilitating impact on the Presidential Inauguration. As an example of these briefings, on January 9, 2013, the CIPSC conducted an unclassified briefing for the DHS Assistant Secretary of IP and numerous utility CEOs on upcoming activities for the Inauguration.

Additional components of Inauguration threat information sharing were the briefings and trainings that PSAs provided to critical infrastructure owners and operators. IP, in conjunction with the USSS, identified critical infrastructure systems and sites that supported Inaugural activities and associated participants. PSAs in the NCR then connected with relevant critical infrastructure owners/operators and conducted assessments or leveraged previous assessments of key critical infrastructure sites and locations in the NCR. This helped owners and operators prepare for Inaugural events and provided principal Federal departments and agencies with information on the preparedness status of key critical infrastructure. The following are some examples of critical infrastructure tools, assessments, and plans used:

- Geospatial Map books
- Infrastructure Survey Tool (IST) security surveys
- Infrastructure Visualization Platforms (IVP), formerly Computer Based Assessment Tool (CBAT)

PSAs also worked with the Office for Bombing Prevention (OBP) to provide training for 275 members of government and NCR private sector organizations, including critical infrastructure owners/operators, such as DC Water. This training included a variety of different courses on security-related topics, such as soft-target awareness, improvised explosive detection, and active shooter preparation.

4.4.3 Threat Information Sharing Activities during the Event

4.4.3.1 DHS – United States Secret Service (USSS) Multi-Agency Coordination Center (MACC)

During the Inaugural events, threat information was also shared by personnel supporting various Federal, State, and local operations and command centers. The DHS-IP Desk located in the USSS-operated Multi-Agency Coordination Center (MACC) was the primary coordination center for PSA activities related to Inaugural events. It provided 24-hour coverage. The DHS-IP Desk in the USSS Critical Infrastructure Coordination Center (CICC) served as the alternate coordination center.

The CICC housed representatives from 27 private sector entities during the Inauguration. PSAs used a range of formal and informal processes to share information. These included in-person communication with critical infrastructure representatives sitting in the CICC, phone calls, and emails to share information about threats to critical infrastructure with critical infrastructure owners/operators. They were prepared to coordinate with the USSS and the FBI to share information had the need arose. The CICC also provided reporting to the MACC, the National Infrastructure Coordinating Center (NICC), and DHS Operations.

The NICC Watch and Warning maintained its 24x7 steady state operations. PSAs used Spot Reports (SPOTREP) to share information with the NICC and IP Operations when needed and to provide updates on the status of critical infrastructure incidents.

4.4.3.2 DHS – Office of Intelligence and Analysis

I&A Field Operations Mid-Atlantic Region and I&A Intelligence Watch and Warning supported the event by reporting and sharing emerging incident threat information pertaining to the event with DHS headquarters and State and local partners, including providing SPOTREPs. I&A Field Operations Mid-Atlantic Region also deployed Intelligence Officers to the FBI Counterterrorism Operations Center (CTOC) and Washington, D.C. and VA Emergency Operations Centers (EOCs) in order to augment DHS support and coordination with Federal, State, local, tribal, territorial, and private sector partners during the NSSE.

4.4.3.3 DHS – NCCIC

The National Cybersecurity and Communications Integration Center's (NCCIC) National Coordinating Center (NCC) provided direct and indirect support for the Inauguration through coordination and collaboration with the Communications Sector. It also supported coordination and communication between Federal and industry constituent members of the Communications Information Sharing and Analysis Center (ISAC) (which is the NCC) regarding operational issues and incidents of concern.

4.4.3.4 DHS – NOC

The National Operations Center (NOC) tracked Inaugural events at the Awareness level, from January 20-22. The Crisis Action Team (CAT) was activated at NOC-Watch with event-tailored staffing to provide support on Inauguration Day.

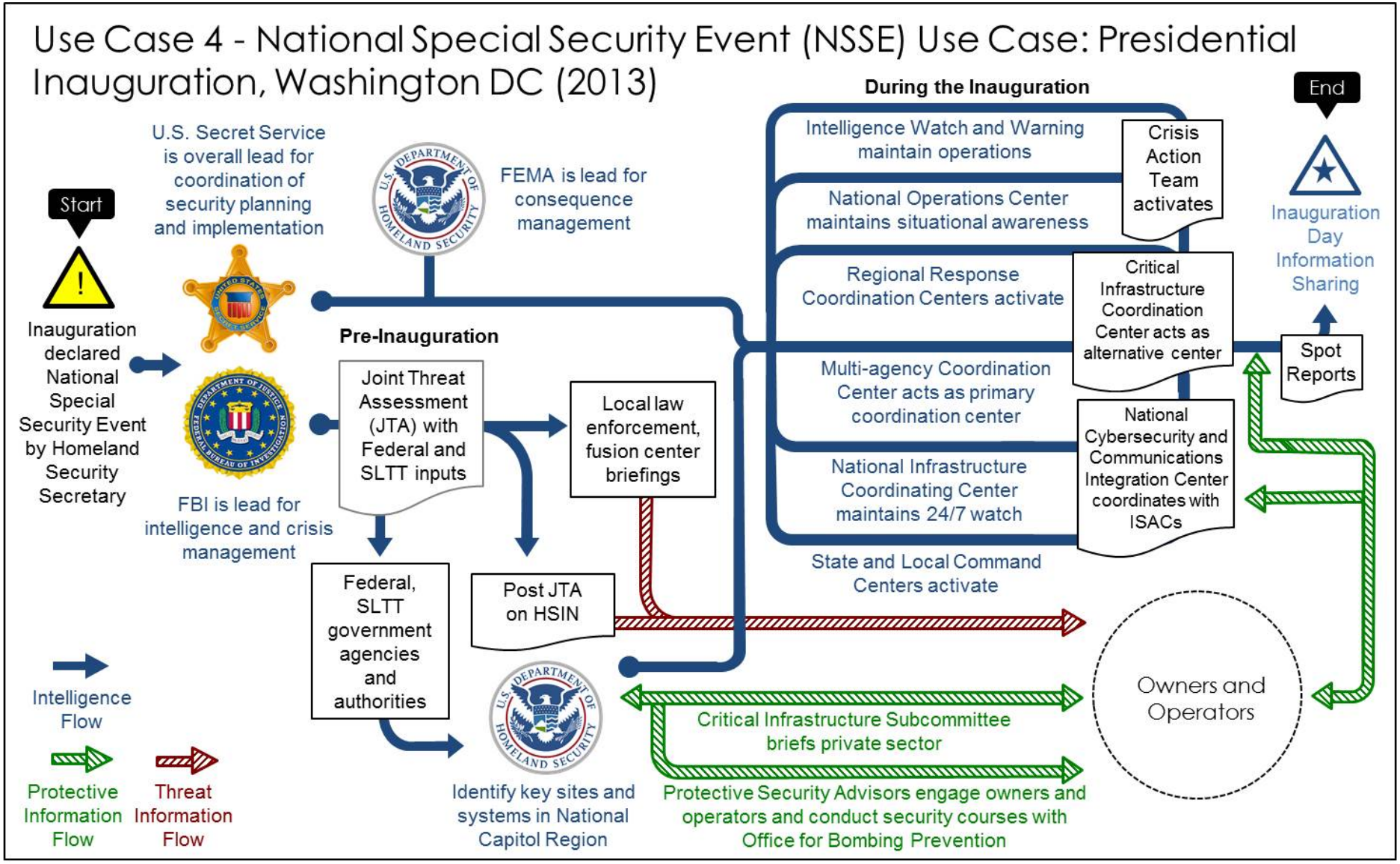


Figure 12: Use Case 4 – National Special Security Event (NSSE) Use Case: Presidential Inauguration, Washington, DC (2013)

Page intentionally left blank.

List of Acronyms

AIS	Automated Indicator Sharing
AMSC	Area Maritime Security Committees (U.S. Coast Guard – Department of Homeland Security)
AMSP	Area Maritime Security Plan
AOR	Areas of Responsibility
ATIX	Automated Trusted Information Exchange
C3	Critical Infrastructure Cyber Community
CAT	Crisis Action Team
CBAT	Computer-Based Assessment Tool (now the Infrastructure Visualization Platform [IVP])
CCTV	Closed-Circuit Television
CG-FAC	Coast Guard Office of Port and Facility Compliance
CICC	Critical Infrastructure Coordination Center
CIF	Classified Intelligence Forum for the Private Sector
CIG	Financial Sector Cyber Intelligence Group
CIMS	Contact Information Management System
CIPAC	Critical Infrastructure Partnership Advisory Council
CIPSC	Critical Infrastructure Protection Sub-Committee
CISCP	Cyber Information Sharing and Collaboration Program
CMC	Crisis Management Center
COP	Common Operating Picture
COTP	Caption of the Port
CS&C	Office of Cybersecurity and Communications (Department of Homeland Security)
CSA	Cyber Security Advisor
CSO	Chief Security Officer
CTAB	Counter Terrorism Advisory Board
CTOC	Counterterrorism Operations Center
DFIR	Daily Field Information Report (formerly Strategic Transportation Threat Awareness Report [STTAR])
DHS	Department of Homeland Security
DOD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
DOT	Department of Transportation
DSAC	Domestic Security Alliance Council
EEI	Edison Electric Institute
EOC	Emergency Operations Center
EPA	Environmental Protection Agency
EWG	Engagement Working Group
FAR	Field Analysis Report
FBI	Federal Bureau of Investigation (Department of Justice)
FCC	Federal Communications Commission
FDA	Food and Drug Administration (FDA)
FEMA	Federal Emergency Management Agency (Department of Homeland Security)
FERC	Federal Energy Regulatory Commission
FIO	Field Intelligence Officer (Department of Homeland Security)
FLASH	FBI Liaison Alert System
FOUO	For Official Use Only
FSLC	Federal Senior Leadership Council
GCC	Government Coordinating Council
GSA	General Services Administration
HHS	Health and Human Services
HMI	Human-Machine Interface
HSDN	Homeland Secure Data Network
HSI	Homeland Security Investigations
HSIN	Homeland Security Information Network (Department of Homeland Security)
I&A	Office of Intelligence and Analysis (Department of Homeland Security)
IC	Intelligence Community
IC3	Internet Crime Complaint Center (Federal Bureau of Investigation)
ICS	Industrial Control System
ICS-CERT	Industrial Control System Cyber Emergency Response Team (Department of Homeland Security, Office of Cybersecurity and Communications)
IED	Improvised Explosive Device
IEMC	Integrated Emergency Management Course
IIB	Intelligence Integration Branch
IIR	Intelligence Information Report
IO	Intelligence Officer
IP	Office of Infrastructure Protection (Department of Homeland Security, National Protection and Programs Directorate)

ISA-IPC	Information Sharing and Access Interagency Policy Committee
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organization
ISAO-SO	Information Sharing and Analysis Organization – Standards Organization
ISC	Interagency Security Committee
ISE	Information Sharing Environment
IST	Infrastructure Survey Tool (Department of Homeland Security)
IT	Information Technology
IVP	Infrastructure Visualization Platform (formerly the Computer-Based Assessment Tool [CBAT]) (Department of Homeland Security)
IWW	Intelligence Watch and Warning Division (Department of Homeland Security)
JCAT	Joint Counterterrorism Assessment Team
JCTAWS	Joint Counterterrorism Awareness Workshop Series
JIB	Joint Intelligence Bulletin
JTA	Joint Threat Assessment
JTTF	Joint Terrorism Task Force
JWICS	Joint Worldwide Intelligence Communication Systems
LEEP	Law Enforcement Enterprise Portal (Federal Bureau of Investigation)
LES	Law Enforcement Sensitive
MACC	Multi-Agency Coordination Center
MS-ISAC	Multi-State – Information Sharing and Analysis Center
NBEOC	National Business Emergency Operations Center (Department of Homeland Security, Federal Emergency Management Agency)
NCATS	National Cybersecurity Assessment and Technical Services
NCC	National Coordinating Center for Communications (Department of Homeland Security)
NCCIC	National Cybersecurity and Communications Integration Center (Department of Homeland Security, Office of Cybersecurity and Communications)
NCI	National Council of Information Sharing and Analysis Centers
NCR	National Capital Region
NCRIC	Northern California Regional Intelligence Center
NCSC	National Counterintelligence and Security Center
NCTC	National Counterterrorism Center
NGO	Nongovernmental Organization
NICC	National Infrastructure Coordinating Center (Department of Homeland Security, Office of Infrastructure Protection)
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NOC	National Operations Center (Department of Homeland Security)
NPPD	National Protection and Programs Directorate (Department of Homeland Security)
NRC	Nuclear Regulatory Commission or National Response Center
NS/EP	National security and emergency preparedness
NSI	National Suspicious Activity Report (SAR) Initiative
NSIS	National Strategy for Information Sharing
NSISS	National Strategy for Information Sharing and Safeguarding
NSSE	National Special Security Event
NTIPA	National Threat Identification and Prioritization Assessment
NWC	National Watch Center (Department of Homeland Security, Federal Emergency Management Agency)
OBP	Office for Bombing Prevention (Department of Homeland Security, Office of Infrastructure Protection)
OCIA	Office of Cyber and Infrastructure Analysis (Department of Homeland Security)
OCIO	Office of Chief Information Officer
ODNI	Office of the Director of National Intelligence
OE	Office of Electricity Delivery and Energy Reliability (Department of Energy)
OEC	Office of Emergency Communications (Department of Homeland Security)
OHSEC	Office of Homeland Security and Emergency Coordination (United States Department of Agriculture)
OSAC	Overseas Security Advisory Council
PCII	Protected Critical Infrastructure Information
PG&E	Pacific Gas and Electric
PII	Personally Identifiable Information
PIN	Private Industry Notification
PM-ISE	Program Manager for the Information Sharing Environment (Office of the Director of National Intelligence)
PPD-21	Presidential Policy Directive 21

PSA Protective Security Advisor (Department of Homeland Security, Office of Infrastructure Protection)

PSAP Public Safety Answering Points

PSCD Protective Security Coordination Division (Department of Homeland Security, Office of Infrastructure Protection)

PSHSB Public Safety and Homeland Security Bureau (Federal Communications Commission)

RC3 Regional Consortium Coordinating Council

RD Regional Director (Department of Homeland Security, Office of Infrastructure Protection)

RE-ISAC Real Estate – Infrastructure Sharing and Analysis Center

RFI Request for Information

RISS Regional Information Sharing Systems

RRAP Regional Resiliency Assessment Program (Department of Homeland Security)

SAIC Strategic Analysis and Information Center

SAR Suspicious Activity Reporting

SCC Sector Coordinating Council

SEAR Special Event Activity Rating

SECIR Stakeholder Engagement and Cyber Infrastructure Resilience Division (Department of Homeland Security, Office of Cybersecurity and Communications)

SLTT State, local, tribal, and territorial

SLTTGCC State, Local, Tribal and Territorial Government Coordinating Council

SME Subject Matter Expert

SOC Secretary's Operations Center (Health and Human Services)

SOP Standard Operating Procedure

SOPD Sector Outreach and Programs Division (Department of Homeland Security, Office of Infrastructure Protection)

SPOTREP Spot Reports

SSA Sector-Specific Agency

SSI Sensitive Security Information

STIX Structured Threat Information eXpression

STTAR Strategic Transportation Threat Awareness Report (now the Daily Field Information Report [DFIR])

SVTC Secure Video Teleconference

TAXII Trusted Automated eXchange of Indicator Information

TLP Traffic Light Protocol

TRACE MOVI Transportation Security Administration Remote Access to Classified Enclaves (MOVI is a vendor name)

TS/SCI Top Secret/Sensitive Compartmented Information

TSA Transportation Security Administration (Department of Homeland Security)

TSC Terrorist Security Center (Federal Bureau of Investigation)

TSOC Transportation Security Administration (TSA) Operations Center (Department of Homeland Security)

TTP Tactics, Techniques, and Procedures

U//FOUO Unclassified//For Official Use Only

US-CERT United States Computer Emergency Response Team (Department of Homeland Security, Office of Cybersecurity and Communications)

USCG United States Coast Guard (Department of Homeland Security)

USDA United States Department of Agriculture

USG United States Government

USSS United States Secret Service (Department of Homeland Security)

WOW Waves on the Waterfront (U.S. Coast Guard – Department of Homeland Security)

Page intentionally left blank.

Appendix A: Federal Operations Centers[68, 69]

Federal departments and agencies use their organizational operation/watch centers to meet internal information sharing requirements relating to critical infrastructure security and resilience situational awareness. These operations centers also often communicate directly with owners and operators within their sector, though some communicate primarily during disasters. The table that follows includes their roles, responsibilities, and points of contact.

Agency/Org	Office/Center	Roles/Responsibilities/Scope	When to Contact	Phone/Email	Website
Department of Energy (DOE)	Emergency Ops Center (EOC)	The Operations Center provides 24-hour-a-day situational awareness, alert, warning, and notifications on events and incidents impacting the DOE/National Nuclear Security Administration mission space.	24/7	Primary POC: (202) 586-8100 Unclassified: doehqeoc@oem.doe.gov Secret: doeeoc@doe.sgov.gov	https://nnsa.energy.gov/aboutus/ourprograms/emergencyoperationscounterterrorism/operationscenter
Department of Health and Human Services (HHS)	Centers for Disease Control and Prevention (CDC) Emergency Operations Center (EOC)	CDC's Emergency Operations Center serves as CDC's command center for monitoring emergency response to public health threats in the United States and abroad. Staffed around-the-clock, the EOC is the central point of contact for reporting public health threats, and supports the Secretary's Operations Center of the U.S. Department of Health and Human Services.	24/7	800-CDC-INFO https://wwwn.cdc.gov/dcs/ContactUs/Form	http://www.cdc.gov/phpr/eoc.htm

[68] Selected from *Critical Infrastructure Security and Resilience Functional Relationships* – DHS, June 2013, including updated information for this Framework, June 2016.

[69] Federal Sector-Specific Operations Centers have varying operational models. Many primarily support their internal agency needs and do not interact directly with critical infrastructure owners and operators, however some do. See entity descriptions for further information.

Agency/Org	Office/Center	Roles/Responsibilities/Scope	When to Contact	Phone/Email	Website
Department of Health and Human Services (HHS)	U.S. Food and Drug Administration (FDA) Emergency Operations Center	The Office of Crisis Management manages FDA's Emergency Operations Center (EOC), activating an Incident Management Group based in the EOC with augmented staffing from relevant centers and offices to monitor emergency situations, triage complaints and alerts, issue mission assignments to organizational components, coordinate overall agency response operations, and communicate with external partners requesting technical and material support.	Major disasters and emergencies	(866) 300-4374	http://www.fda.gov/AboutFDA/CentersOffices/OfficeofOperations/OfficeofCrisisManagement/ucm253409.htm
Department of Homeland Security (DHS)	Federal Emergency Management Agency (FEMA) National Business Emergency Operations Center (NBEOC)	The NBEOC is envisioned as a groundbreaking new virtual organization that serves as FEMA's clearinghouse for two-way information sharing between public and private sector stakeholders in preparing for, responding to, and recovering from disasters. Note: The NBEOC is only in operation during major disasters and emergencies.	Major disasters and emergencies	FEMA-private-sector@dhs.gov FEMA-PSR@dhs.gov	http://www.fema.gov/private-sector
Department of Homeland Security (DHS)	Federal Emergency Management Agency (FEMA) National Watch Center (NWC)	The NWC supports the collection and distribution of pre-incident information to the DHS National Operations Center (NOC) for the development of a national Common Operating Picture (COP).	24/7	(202)-646-2828 FEMA-NWC@fema.gov	http://on.fema.net/COMPONENTS/ORR/RESPONSE/Pages/NationalWatchCenter.aspx (DHS only)

Agency/Org	Office/Center	Roles/Responsibilities/Scope	When to Contact	Phone/Email	Website
Department of Homeland Security (DHS)	National Coordinating Center for Communications (NCC) (National Cybersecurity and Communications Integration Center [NCCIC] element)	As part of the DHS NCCIC, the NCC continuously monitors national and international incidents and events that may impact emergency communications. Incidents include not only acts of terrorism, but also natural events, such as tornadoes, floods, hurricanes and earthquakes. In cases of emergency, NCC Watch leads emergency communications response and recovery efforts under Emergency Support Function #2 of the National Response Framework. In January 2000, the White House designated NCC as the ISAC for Telecommunications, in accordance with Presidential Decision Directive-63. The NCC-Communications ISAC facilitates the exchange of vulnerability, threat, intrusion, and anomaly information amongst 24 Federal agencies and over 50 private industry sector members, including critical infrastructure owners in trusted environment(s), to support the NCC's national security/emergency preparedness communications mission.	24/7 Notify on any current or projected communications outages, threats, vulnerabilities, and/or other critical communications problems and/or concerns.	(703) 235-5080 Unclassified: ncc@hq.dhs.gov Secret: ncc@dhs.sgov.gov JWICS: ncc@dhs.ic.gov	www.dhs.gov/national-coordinating-center-telecommunications
Department of Homeland Security (DHS)	National Operations Center (NOC) NOC Watch I&A Intelligence Watch and Warning Branch (IWW)	Through the NOC, the office provides real-time situational awareness and monitoring of the homeland, coordinates incidents and response activities, and, in conjunction with the Office of Intelligence and Analysis (I&A), Intelligence Watch and Warning Branch issues advisories and bulletins concerning threats to homeland security, as well as specific protective measures.	24/7	(202) 282-8101 State and Local Desk: (202) 282-9685 Requests for Information: DHS-SPS-RFI@hq.dhs.gov NOC Desk Officer can answer questions about current events and relay information to DHS Intelligence Officers assigned to fusion centers: NOC.State&Local@hq.dhs.gov IA.IWW@hq.dhs.gov	www.dhs.gov/about-office-operations-coordination-and-planning https://hsin.dhs.gov

Agency/Org	Office/Center	Roles/Responsibilities/Scope	When to Contact	Phone/Email	Website
Department of Homeland Security (DHS)	Transportation Security Administration (TSA) Operations Center (TSOC)	The TSOC is a sophisticated, 24-7 operations center that maintains continuous information sharing with Federal, State, local, and tribal transportation-related entities. It serves as a single point of contact for security-related incidents or crises in all modes of transportation and is the primary interface to the DHS NOC.	24/7	(703) 563-3236 TSOC.ST@dhs.gov	https://www.tsa.gov/file/inside-look-transportation-security-operations-center
Department of Homeland Security (DHS)	U.S. Coast Guard National Response Center	The Coast Guard Office of Port and Facility Compliance (Commandant CG-FAC) develops and implements programs to prevent safety, security, and environmental incidents in the maritime arena and to protect continued vitality of the Marine Transportation System. Contact this office for routine concerns regarding critical infrastructure policy. To report a maritime critical infrastructure incident, including oil spills and chemical releases, after calling 911, please contact the National Response Center (NRC).	24/7	CG-FAC: (202) 267-2675 NRC: (800) 424-8802	http://www.nrc.uscg.mil/
Department of Transportation (DOT)	Crisis Management Center (CMC)	The CMC is designed to monitor the Nation's transportation systems and infrastructure 24 hours a day, 7 days a week. In the event of a disaster it serves as the DOT's interagency liaison with the Federal Government and SLTT governments as appropriate.	24/7	(202) 366-1863 cmc-01@dot.gov	https://www.transportation.gov/mission/administrations/intelligence-security-emergency-response/operations-division
Environmental Protection Agency (EPA)	Emergency Operations Center (EOC)	The EPA Emergency Operations Center (EOC) serves as EPA's emergency response operational focal point. It is a communication and coordination hub designed to increase data management and coordination capabilities.	24/7	202-564-3850 eoc.epahq@epa.gov	http://www.epa.gov/emergency-response/emergency-operation-center

Agency/Org	Office/Center	Roles/Responsibilities/Scope	When to Contact	Phone/Email	Website
Federal Communications Commission (FCC)	Public Safety and Homeland Security Bureau (PSHSB) Operations Center	The PSHSB Operations Center provides 24-hour situational awareness and strategic assessments on trends for crisis scenarios that may have public safety, national security, or emergency preparedness implications, and serves as the primary communications center for the FCC. The Public Safety Support Center online portal enables Public Safety Answering Points (PSAPs), also known as 911 Call Centers, and other Public Safety entities, to request support from the Public Safety and Homeland Security Bureau and to notify it of problems or issues impacting the provision of emergency services.	24/7	Unclassified: (202) 418-1122 TS/SCI STE: (202) 418-1192 TS/SCI FAX: (202) 418-0908 Unclassified: FCCOPCenter@fcc.gov Secret: FCCOPS@adnet.sgov.gov TS: FCCOPS@gold.ic.gov	FCC Operations Center https://www.fcc.gov/general/operations-center-public-safety-homeland-security-bureau Public Safety Support Center https://www.fcc.gov/general/public-safety-support-center
United States Department of Agriculture (USDA)	Emergency Programs Division Operations Center	The Emergency Programs Division operates the Operations Center, the USDA focal point for all emergency management and coordination at the USDA headquarters. The Center monitors international, national, and local news for items that may impact USDA and is the primary USDA entry point for emergency information from operations centers external to USDA.	24/7	(202) 720-5711 Request to be connected to the Food/Ag Sector lead in the USDA Office of Homeland Security and Emergency Coordination (OHSEC) opscenter@dm.usda.gov	http://www.dm.usda.gov/ohsec/epd/
United States Nuclear Regulatory Commission (NRC)	NRC Operations Center	The primary center of communication and coordination among the NRC, its licensees, State and tribal agencies, and other Federal agencies, regarding operating events involving nuclear reactors or materials.	24/7	(301) 816-5100 HOO.HOC@nrc.gov	http://www.nrc.gov

Page intentionally left blank.

Appendix B: Other Threat Information Sharing Entities Not Included in Section 3.0 or Appendix A

Entity	Roles/Responsibilities/Scope	Phone/Email	Website
Financial Sector Cyber Intelligence Group (CIG)	The CIG monitors and analyzes all-source intelligence on cyber threats to the financial sector; provides timely, actionable cyber threat information to the sector; and solicits feedback and information requirements from the sector.	cig@treasury.gov	
Office of the Program Manager for the Information Sharing Environment (PM-ISE)	The role of PM-ISE is to coordinate and facilitate the development of a network-centric information-sharing environment for terrorism and homeland security information by focusing on standards and architecture, security and access, associated privacy protections, and best practices. PM-ISE serves as a change agent and center for innovation and discovery in providing ideas, tools, and resources to mission partners who then apply them to their own agencies or communities.	(202) 331-4060 ISE-public-affairs@dni.gov	www.ise.gov
Threat Management Division	The Federal Protective Service, Threat Management Division provides mission partners, tenants, and stakeholders with threat-based, mission-focused analysis of current and emerging threats to government facilities and their occupants across the nation.	202-732-8200 FPS-INTEL@hq.dhs.gov	
National Explosives Task Force (NETF)	The mission of NETF is to coordinate the rapid integration of explosives expertise with intelligence and law enforcement information in order to support operational decisions by those responsible for preventing terrorist or criminal use of explosives. The NETF has three major goals: improve domestic explosives domain awareness, integrate explosives intelligence and expertise into investigations, and coordinate improvised explosive devices (IED)-related publications. The NETF supports the “whole of Government” approach to address gaps in the coordination and consolidation of efforts in the response to explosives incidents. The NETF also works with the Joint Program Office for Countering IEDs to align its mission, resources, and expertise with the U.S. Policy Statement on Countering Improvised Explosives Devices. The NETF is staffed with bomb technicians, investigators, and intelligence analysts from the FBI; Bureau of Alcohol, Tobacco, Firearms, and Explosives; the Department of Homeland Security Office for Bombing Prevention and Transportation Security Administration; the Office of the Director of National Intelligence National Counterterrorism Center; the Department of Defense (DoD); and the Terrorist Explosive Device Analytical Center.	NETF@ic.fbi.gov	

Page intentionally left blank.

Appendix C: Entities with Critical Infrastructure Security and Resilience Program, Policy, and Mitigation Responsibilities

In addition to the threat information-sharing entities categorized in Section 2.2 and those included in Appendix A and B, there are entities with significant responsibilities for critical infrastructure security and resilience related policies and programs. They coordinate with the critical infrastructure community and develop or coordinate the development of strategies, policies, plans, and standards for the critical infrastructure security and resilience mission. During heightened threats or incident response, they may serve as subject matter experts to the entities mainly responsible for threat information sharing and analysis. They may also coordinate and develop resources and tools to assist critical infrastructure owners and operators in addressing emerging threats. Typically, these entities are consumers of the information provided by the information-sharing hubs described above and may provide information to or receive information from the information-sharing hubs. In some cases, they may also share threat information directly with stakeholders prior to or during an incident, but 24/7 “threat information sharing” is not one of their core responsibilities. This appendix is not exhaustive.

Entity	Roles/Responsibilities/Scope	Phone/Email	Website
Critical Infrastructure Cyber Community (C3) Voluntary Program	The C3 Voluntary Program is an innovative public-private partnership led by DHS to help align critical infrastructure owners and operators with existing resources that will assist them in using the National Institute of Standards and Technology (NIST) Cybersecurity Framework to manage their cyber risks. The primary way this is achieved is through providing a central repository of resources on its website and holding webinars and events across the country.	CCubedVP@hq.dhs.gov	www.US-CERT.gov/CCubedVP

Entity	Roles/Responsibilities/Scope	Phone/Email	Website
DHS-National Protection and Programs Directorate (NPPD) Office of Cybersecurity and Communications (CS&C)	CS&C is responsible for enhancing the security, resilience, and reliability of the Nation's cyber and communications infrastructure. CS&C actively engages the public and private sectors as well as international partners to prepare for, prevent, and respond to catastrophic incidents that could degrade or overwhelm these strategic assets. CS&C carries out its mission through its five divisions including: • The NCCIC see entity description on page 31 • The Stakeholder Engagement and Cyber Infrastructure Resilience (SECIR) division and field personnel, Cyber Security Advisors (CSAs). CSAs act as principal field liaisons in cybersecurity and provide a Federal resource to regions, communities, and businesses. CSAs will work with established programs in State and local areas, such as Protective Security Advisors (PSAs), Federal Emergency Management Agency (FEMA) emergency management personnel, and fusion center personnel. • The Office of Emergency Communications (OEC) supports and promotes communications used by emergency responders and government officials to keep America safe, secure, and resilient. The office leads the Nation's operable and interoperable public safety and national security and emergency preparedness (NS/EP) communications efforts. OEC provides training, coordination, tools, and guidance to help its Federal, State, local, tribal, territorial, and industry partners develop their emergency communications capabilities.	CSA Program: CSE@dhs.gov OEC: OEC@dhs.gov	https://www.dhs.gov/office-cybersecurity-and-communications
DHS-NPPD Office of Infrastructure Protection (IP)	IP leads and coordinates national programs and policies on critical infrastructure security and resilience and has established strong partnerships across the public and private sectors. The office conducts and facilitates vulnerability and consequence assessments to help critical infrastructure owners and operators and State, local, tribal, and territorial (SLTT) partners understand and address risks to critical infrastructure. IP provides information on emerging threats and hazards so that appropriate actions can be taken. The office also offers tools and training to partners to help them manage the risks to their assets, systems, and networks. IP carries out its mission through its five divisions, which include the National Infrastructure Coordinating Center (NICC) and Protective Security Advisor (PSA) field personnel. See IP's website for more information.		https://www.dhs.gov/office-infrastructure-protection

Entity	Roles/Responsibilities/Scope	Phone/Email	Website
National Counterintelligence and Security Center (NCSC)	NCSC leads and supports the integration of counterintelligence and security activities of the U.S. Government, the Intelligence Community and private sector entities at risk from intelligence collection or penetration by foreign or other adversaries. Foreign adversaries pose an ongoing threat to U.S. critical infrastructure with the possibility of doing serious damage to the U.S. economy and national security. NCSC is responsible for producing in consultation with appropriate U.S. Government departments and agencies and private sector entities, the National Threat Identification and Prioritization Assessment (NTIPA), which provides guidance for programs and activities that guard against foreign penetrations of the U.S. Government. NCSC initiatives include insider threat programs, supply chain risk management, and other security measures relevant to critical infrastructure protection.		https://www.ncsc.gov/
Sector-Specific Agencies (SSAs)	See entity description in Section 3 on page 40		

Page intentionally left blank.

Appendix D: Threat Information Products

This appendix provides information on a number of different specific threat information products. This list is not exhaustive, but is geared toward threat information products aimed at or which often get passed on to owners and operators, or reference infrastructure.

Name of Source	Description	Organization Producing	Classification	Website
Alerts – through the National Cybersecurity and Communications Integration Center's (NCCIC) ICS portal (Control System Compartment) or the enterprise systems portal (Cobalt Compartment)	Alerts are used by the NCCIC and its partners when they want to share threat level information, but are working with intelligence and law enforcement to limit the amount of information that could be leveraged by adversaries.	NCCIC	U//FOUO or Classified	
Financial Sector Cyber Intelligence Group (CIG) Circulars	CIG Circulars are for the network security specialists of financial institutions, their cybersecurity service providers, and other critical infrastructure partners. They provide information on cyber actors' tactics, techniques, procedures, and associated indicators, and are used to support network defense capabilities and planning.	Treasury, Office of Critical Infrastructure Protection, Financial Sector Cyber Intelligence Group	Unclassified	http://fsisac.com In addition, eligible stakeholders can download CIG Circulars from the DHS Homeland Security Information Network (HSIN) Financial Services portal. For information on membership, download the quick guide from: http://go.usa.gov/3YH45
Daily Report	Daily Reports are compiled by using multiple open-source and subscription-based intelligence providers. After incidents, they can be used to provide awareness of threats to members, partners and across sectors to other Information Sharing and Analysis Centers (ISACs).	RE-ISAC	Unclassified	
DHS Daily Open Source Infrastructure Report	The DHS Daily Open Source Infrastructure Report is collected each business day as a summary of open-source published information concerning significant critical infrastructure issues. Each Daily Report is divided by the critical infrastructure sectors and key assets defined in the National Infrastructure Protection Plan.	DHS-IP	Unclassified	http://www.dhs.gov/publication/daily-open-source-infrastructure-report

Name of Source	Description	Organization Producing	Classification	Website
Information Bulletin (IB)	Information Bulletins (IB) are a versatile, analytical document that captures and reports key information that is unclassified. The Information Bulletin covers a wide array of topics, including, but not limited to, assessments of upcoming events impacting federal facilities and analysis of region specific terrorism concerns.	DHS Federal Protective Services		
Executive Security Briefing (ESB)	Executive Security Briefings (ESBs) provide regional leadership and stakeholders with analytical support that enhances daily operations by providing situational awareness and decision support. They focus on providing analytically-enhanced decision support for a time sensitive, topic-specific threats.	DHS Federal Protective Services		
DHS Terrorism Report	These Reports are posted to Homeland Security Information Network – Critical Infrastructure (HSIN-CI), along with the Joint Intelligence Bulletins and Field Analysis Reports. They look at changes to threat situations and are used to highlight the need for vigilance. In the aftermath of an incident, one Report included audio recording from the Critical Infrastructure Stakeholder Teleconference Call, which provided the government and owners and operators with a forum to share incident- and threat-specific information.	DHS-IP-NICC	Classified and Unclassified	
FBI Liaison Alert System (FLASH) Messages	FLASH is used to share details and information with the private sector. FLASH messages are used to release industry-specific details on current and emerging threat trends and technical indicators to private sector partners.	FBI		Please contact the FBI with any questions related to FLASH reports at either your local CTF or FBI CYWATCH: Email: cywatch@ic.fbi.gov or Voice: +1-855-292-3937
Field Analysis Report (FAR)	FARs are the finished analysis products that can look at threats and impacts on critical infrastructure in a particular region. They contain analysis based on evidence and research gathered from technical open source reports from multiple sources inside and outside of government. Posted to HSIN-CI, these reports, along with the Joint Intelligence Bulletins and DHS Terrorism Reports, look at increased threat situations and the need for vigilance. Examples of previous postings have been used to provide the government and critical infrastructure owners and operators with a forum to share incident- and threat-specific information. Some previous postings included audio recordings from the Critical Infrastructure Stakeholder Teleconference Call.	DHS-I&A	Classified and Unclassified	

Name of Source	Description	Organization Producing	Classification	Website
Intelligence Information Reports (IIRs)	IIRs are published by DHS-Office of Intelligence and Analysis (I&A) to share details on various threats, and they are shared with the Intelligence Community. For example, I&A published a number of IIRs detailing malware campaigns against State, local, and private sector facilities.	DHS-I&A	Classified and Unclassified	
Joint Intelligence Bulletin (JIB)	The JIB provides timely information or analysis on a recent or current event or development of interest. It is shared with information and analysis customers, and can be produced at various classification levels. It focuses on Homeland Security issues, is written on an ad hoc basis, and is generally one to three pages. It is available on HSIN or the Homeland Secure Data Network (HSDN), depending on the classification of the information.[70]	FBI, DHS-I&A	Various	
Joint Threat Assessment (JTA)	JTAs are produced by members of the intelligence community. A JTA addresses international and domestic terrorist, criminal, cyber, and transportation-related threats to National Special Security Events (NSSEs) or assets. Once produced, JTAs can be shared with Federal, state, and local government agencies and authorities to help them develop and prioritize protective and support measures. JTAs can be shared widely with NCR critical infrastructure owners/operators through the HSIN, local law enforcement, fusion centers, and unclassified and classified briefings.	FBI		
National Counterterrorism Center (NCTC) Counterterrorism Digest (CT Digest)	NCTC CT Digest is a compendium of international and domestic news focusing on counterterrorism information. It is available on HSIN-CI, InfraGard, and the Domestic Security Alliance Council (DSAC). CT Digest also contains assessments from seasoned analysts and first responders.	NCTC		Find on HSIN-CI, InfraGard, and DSAC
Private Industry Notifications (PINs)	PINs release industry-specific details on current and emerging threat trends and technical indicators to the private sector.	FBI		

[70] Intelligence Guide for First Responders, 2nd edition, Interagency Threat Assessment and Coordination Group (2011).

Name of Source	Description	Organization Producing	Classification	Website
Suspicious Activity Report (SAR)	The Nationwide SAR Initiative (NSI) is a collaborative effort led by the U.S. Department of Justice (DOJ), Bureau of Justice Assistance, in partnership with DHS, the FBI, and State, local, tribal, and territorial law enforcement partners. This initiative provides law enforcement with another tool to help prevent terrorism and other terrorism-related crime. It establishes a national capacity for gathering, documenting, processing, analyzing, and sharing SAR information. The NSI is a standardized process—including stakeholder outreach, privacy protections, training, and facilitation of technology—for identifying and reporting suspicious activity in jurisdictions across the country, and it also serves as the unified focal point for sharing SAR information.	Owners/Operators/ Private Sector, DHS, FBI, SLTT law enforcement partners	Classified and Unclassified	http://www.dhs.gov/how-do-i/report-suspicious-activity https://www.ise.gov/
Spot Reports (SPOTREP)	Spot Reports can be used to share necessary information with the NICC and IP Operations and to provide updates on the status of critical infrastructure incidents.	DHS-IP-NICC	Classified and Unclassified	

Appendix E: Threat Information Mechanisms and Sources, and Tools to Assess Threats

This appendix provides information on a number of different specific mechanisms and sources of threat information. These specific sources of information complement the traditional sharing of information through standard communications channels, including emails, in-person briefings, teleconferences, bulletins, reports, web portals, and emergency operations centers.

Name of Source	Description	Organization Producing	Classification	Website
Cobalt Compartment (US-CERT)	The Cobalt Compartment is National Cybersecurity and Communications Integration Center's (NCCIC) secure portal for sharing information on cyber threats to enterprise systems.	DHS-NCCIC		http://www.dhs.gov/publication/connecting-nicc-and-nccic
Control System Compartment (ICS-CERT)	The Control System Compartment is NCCIC's secure portal for sharing information on cyber threats for industrial control systems (ICS) owners and operators.	DHS-NCCIC		http://www.dhs.gov/publication/connecting-nicc-and-nccic
Classified Intelligence Forums (CIFs)	CIFs are an engagement with appropriately cleared and identified private sector critical infrastructure representatives within the Commercial Facilities Sector and the Cross Sector Coordinating Council. They are conducted bimonthly at DHS Headquarters, and have been expanded regionally to solicit feedback from private sector representatives, which can help to inform the development of current and future intelligence products and other appropriate information sharing or analytic initiatives.	DHS I&A; DHS NPPD	Several classes, but normally U//FOUO	
DHS Daily Open Source Infrastructure Report	The DHS Daily Open Source Infrastructure Report is collected each business day as a summary of open-source published information concerning significant critical infrastructure issues. Each Daily Report is divided by the critical infrastructure sectors and key assets defined in the National Infrastructure Protection Plan.	DHS-IP	Unclassified	http://www.dhs.gov/publication/daily-open-source-infrastructure-report
DHS-Office of Infrastructure Protection (IP) Desk	The DHS-IP Desk is located within the Multi-Agency Coordination Center (MACC), which is run by United States Secret Service (USSS). It serves as the primary coordination center for Protective Security Advisor (PSA) activities during certain National Special Security Events (NSSEs), and provides 24-hour coverage for threat information sharing support.	DHS-IP		

Name of Source	Description	Organization Producing	Classification	Website
DHS Office of Chief Information Officer	The DHS Geospatial Information Infrastructure (GII) provides a Sensitive But Unclassified (SBU)-level platform to host shared geospatial enterprise applications, tools, and information. Available to all users across the entire homeland security/defense enterprise (Federal, State, Local, Tribal and Territories), this capability enables operators and analysts to securely search, discover and access imagery, base maps, DHS operational data, and foundational data; store and share geospatial information in private or public groups; create and share derived geospatial products; access existing common applications and tools such as geocoding; and easily build interactive maps and customized apps for field collection, story maps, and heat maps.	DHS-OCIO	Unclassified	https://gii.dhs.gov/gii
Homeland Security Geospatial Concept of Operations (HSE Geo CONOPS)	The HSE GeoCONOPS is a community-wide resources that allows mission partners to identify existing geospatial resources and capabilities to aid in mission planning and support (i.e. mission blueprint), easily search and discover geospatial data or products available to their mission, and understand how the geospatial community interacts/coordinates to support a diverse mission set through use cases. Through the HSE GeoCONOPs analysts can search, discover, and leverage other geospatial information on critical infrastructure available from other agencies.	DHS OCIO	Unclassified	https://cms.geoplatform.gov/geoconops/
eGuardian	eGuardian is a counterterrorism threat tracking system that is connected to the National Network of Fusion Centers. eGuardian is designed to be used by Federal, State, local, tribal, and territorial law enforcement agencies and local and State fusion centers. eGuardian is also used by Department of Defense as their sole suspicious activity reporting mechanism. Participating agencies are able to provide, view, and analyze Suspicious Activity Reports (SARs) and other terrorism-related information using advanced searching capabilities and geospatial overlays.	FBI	Classified and Unclassified	https://www.fbi.gov/stats-services/eguardian
Email	Email is a key mechanism for information sharing. One can sign up for email alerts, notifications, notification of an upcoming threat call, etc.	Multiple	Classified and Unclassified	
Engagement Working Group (EWG)	EWGs bring potentially affected private sector partners together with representatives from the government to discuss a specific threat or issue. They are created to augment Office of Infrastructure Protection (IP)-Sector Outreach and Programs Division's (SOPD) typical role of facilitating private sector relationships through the Critical Infrastructure Partnership Advisory Council (CIPAC) partnership.	DHS-IP-SOPD	Classified and Unclassified	

Name of Source	Description	Organization Producing	Classification	Website
Homeland Secure Data Network (HSDN)	The HSDN enables classified information to reach Federal agencies that are involved in homeland security missions. HSDN is a classified wide-area network utilized by DHS, DHS Components and other partners, providing effective interconnections to the intelligence community and federal law enforcement resources. Homeland Secure Data Network (HSDN) provides DHS with the ability to collect, disseminate, and exchange both tactical and strategic intelligence and other homeland security information up to the "Secret" level. HSDN also serves as a consolidated backbone that brings together multiple, legacy "Secret" classified networks across the DHS enterprise.	DHS-Office of Chief Information Officer (OCIO)	Classified	
Homeland Security Information Network (HSIN)	The HSIN is the trusted network for homeland security mission operations to share Sensitive But Unclassified information. Federal, State, local, territorial, tribal, international and private sector homeland security partners use HSIN to manage operations, analyze data, send alerts and notices, and in general, share the information they need to do their jobs.	DHS	Unclassified	http://www.dhs.gov/homeland-security-information-network-hsin
Infrastructure Protection Gateway (IP Gateway)	IP Gateway serves as the single interface through which DHS partners can access a large range of information and integrated infrastructure protection data collection, analysis, and response tools to conduct comprehensive vulnerability assessments and risk analysis. It provides one integrated system, streamlining access to the Department's infrastructure protection tools and datasets.	DHS-IP		http://www.dhs.gov/ipgateway
Infrastructure Survey Tool (IST)	The IST is a web-based vulnerability assessment tool conducted by PSAs that applies weighted scores to identify vulnerabilities and trends for specific infrastructure and across the sector. The survey data, composed of weighted scores on a variety of factors for specific critical infrastructure, is graphically displayed in the IST Dashboard that compares the data against similar facilities and informs protective measures, resilience planning, and resource allocation. The resulting survey information is provided to owners and operators and may also be shared with the Sector-Specific Agencies and other Federal, State, local, tribal, and territorial critical infrastructure protection representatives through the interactive dashboards.	DHS-IP's PSAs		https://www.dhs.gov/sites/default/files/publications/ecip-ist-fact-sheet-508.pdf

Name of Source	Description	Organization Producing	Classification	Website
Infrastructure Visualization Platform (IVP) – formerly Computer-Based Assessment Tool (CBAT)	The IVP is a data collection and presentation medium that supports critical infrastructure security, special event planning, and response operations by leveraging assessment data and other relevant materials. The tool integrates assessment data with immersive video, geospatial, and hypermedia data of critical infrastructure facilities, surrounding areas, and transportation routes that assists security personnel in planning, protection, and response efforts. IVP imagery assists infrastructure owners and operators, local law enforcement, and emergency response personnel to prepare for, respond to, and manage critical infrastructure, NSSEs, high-level special events, and contingency operations. IVPs are prepared at the request of facility owners and operators, local law enforcement, and emergency response personnel via the nearest PSA. Depending on the amount of data collected, the IVP team typically takes two weeks to produce a final product, which is a DVD containing self-executing presentation software that is provided to the facility representative, primary stakeholder of a Regional Resiliency Assessment Program (RRAP), or special event security planning personnel. The final products assist these users in training, planning, and in making rapid and informed incident preparedness and management decisions.	DHS-IP's PSAs	FOUO or Protected Critical Infrastructure Information (PCII)	https://www.dhs.gov/infrastructure-visualization-platform
Integrated Emergency Management Course (IEMC)	The IEMC is a four-day course that serves as a training initiative designed to strengthen the ability of local jurisdictions to protect against and respond to a complex coordinated attack. It features briefings (including a threat briefing from the National Counterterrorism Center), case studies, and facilitated discussions based on a community specific attack scenario. Through these scenario-based discussions, participants self-identify gaps in their current operational plans and capabilities as well as possible solutions. Participating private sector partners include representatives from telecommunications/network providers; utilities; major employers—insurance, financial, manufacturing, chemical, logistics, and tourism; hotels; special event venues; downtown business district/chamber representatives; and nonprofit organizations—American Red Cross, Volunteer Organizations Active in Disasters (VOAD), or faith-based networks.	FEMA		https://training.fema.gov/iemc/

Name of Source	Description	Organization Producing	Classification	Website
Joint Counterterrorism Awareness Workshop Series (JCTAWS)	The JCTAWS is a two-day workshop targeting tier one cities. It is designed to improve the ability of local jurisdictions to prepare for, protect against, and respond to complex terrorist attacks. It is designed to strengthen the ability of local jurisdictions to protect against and respond to a complex coordinated attack. It features briefings (including a threat briefing from the National Counterterrorism Center), case studies, and facilitated discussions based on a community specific attack scenario. Through these scenario-based discussions, participants self-identify gaps in their current operational plans and capabilities as well as possible solutions. Since 2010, the JCTAWS workshop has been conducted 20 times with more than 4,500 participants, including telecommunications/network providers; utilities; major employers—insurance, financial, manufacturing, chemical, logistics, and tourism—hotels; special event venues; downtown business district/chamber representatives; and nonprofit organizations—American Red Cross, Volunteer Organizations Active in Disasters (VOAD), or faith-based networks.	NCTC; DHS; FBI		
Law Enforcement Enterprise Portal (LEEP)	The LEEP is an online sharing platform where the FBI posts intelligence information, including both finished intelligence and raw/tactical information. These resources will strengthen case development for investigators, enhance information sharing between agencies, and be accessible in one centralized location.	FBI	Classified or Unclassified	https://www.cjis.gov/CJISEAI/EAIController
Regional Information Sharing Systems (RISS)	RISS offers secure information sharing and communications capabilities, critical analytical and investigative support services, and event deconfliction to enhance officer safety. RISS supports efforts against organized and violent crime, gang activity, drug activity, terrorism, human trafficking, identity theft, and other regional priorities. RISS supports thousands of local, State, Federal, and tribal criminal justice agencies in their efforts to successfully resolve criminal investigations and ensure officer safety. RISS consists of six regional centers and the RISS Technology Support Center.	DOJ Bureau of Justice Assistance		www.riss.net

Name of Source	Description	Organization Producing	Classification	Website
Regional Information Sharing Systems (RISS) Automated Trusted Information Exchange (ATIX)	RISS ATIX provides law enforcement, public safety, and critical infrastructure personnel—representing such entities as public utilities, schools, fire departments, and the chemical industry—with access to homeland security, disaster, and terrorist threat information, as well as secure communication capabilities. There are six regional centers in the nation. The RISS ATIX system includes webpages, discussion forums, secure email, and a document library that can be used to collaborate, share information, and access key resources.	DOJ Bureau of Justice Assistance		www.riss.net/Resources/ATIX
Regional Resiliency Assessment Program (RRAP)	The RRAP is a cooperative assessment of specific critical infrastructure within a designated geographical area and a regional analysis of the surrounding infrastructure led by DHS-NPPD-IP. The RRAP addresses a range of hazards that could have regionally and nationally significant consequences. Each year, the Department selects these voluntary, non-regulatory RRAP projects with input and guidance from Federal and State partners.	DHS-IP		https://www.dhs.gov/regional-resiliency-assessment-program
Request for Information (RFI)	In some cases, Federal agencies request that Information Sharing and Analysis Centers (ISACs) share unclassified information and open source information with their members. Additionally, owners and operators may also be prompted to share with the ISACs any information which they have pertaining to the cases at hand.	ISACs	Unclassified	
Sector and Subsector Information Sharing Working Groups	There are many working groups that participate in information sharing, both public and private. One example is the Dams Sector Information Sharing Working Group, but this is a generic category to illustrate the variety and decentralization inherent in information sharing.	Various	Classified and Unclassified	
Sector-Specific Workshops and Conferences	These workshops and conferences provide a forum for in-person information sharing. They bring together stakeholders from throughout the Federal, State, local, tribal, and territorial spectrum of government agencies, as well as the private sector. They support presentations, briefings, and in-person communications on particular threat or mitigation measures. One example is the Chemical Sector Security Summit, but this is a generic category to illustrate the variety and decentralization inherent in information sharing.	Various	Unclassified	
Sector Threat Briefings	These threat briefings are hosted by a variety of government offices and agencies. They are a means of sharing relevant threat information and findings with private sector owners and operators during times of heightened awareness.	Various	Classified and Unclassified	

Name of Source	Description	Organization Producing	Classification	Website
Secure Video Teleconference (SVTC)	Secure Video Teleconferencing provides a mechanism for government agencies to conduct real-time information sharing conversations and briefings with other government offices and the private sector, as needed.	Government Offices, including DOE and DHS-NICC	Classified	
Special Topic and Targeted Engagements	Special Topic and Targeted Engagements are determined by IP leadership, and occur on various levels, generally when an incident that targets a specific sector is identified. These engagements can be both classified and unclassified. These engagements can be categorized under the Coordination Plan for Targeted Threat and Security Engagements.	DHS-IP	Classified and Unclassified	
Targeted Outreach Campaigns	Targeted Outreach Campaigns are identified in the Coordination Plan for Targeted Threat and Security Engagements as one of the many types of engagements that are conducted with the private sector. These engagements can be both classified and unclassified. Generally outreach campaigns are extensive and conducted around the country to brief on a nationwide threat.	DHS-IP and Cross Sector Council	Classified and Unclassified	
Teleconference (Incident-focused Critical Infrastructure Stakeholder Teleconference)	These teleconferences, led by IP, provide the government and owners and operators with a forum to share incident and threat-specific information. In certain circumstances, audio recordings of the calls have been shared through HSIN-CI.	DHS-IP-NICC	Unclassified	
Transportation Security Administration Remote Access to Classified Enclaves MOVI (TRACE MOVI)	TRACE MOVI is used by government offices to safely share classified information with other government offices and with key private sector partners.	TSA	Classified	
TRIPwire (Technical Resource for Incident Prevention)	TRIPwire is DHS's 24/7 online, collaborative information-sharing network for bomb technicians, first responders, military personnel, government officials, intelligence analysts, and select private sector security professionals to increase awareness of evolving terrorist improvised explosive device (IED) tactics, techniques, and procedures, as well as incident lessons learned and counter-IED preparedness information. It combines expert analyses and reports with relevant documents, images, and videos gathered directly from sources to help users anticipate, identify, and prevent IED incidents. A secure, restricted-access information-sharing network, TRIPwire is available at no cost to registered subscribers and features a publicly accessible homepage with valuable preparedness information for the whole community.	DHS-IP-Office for Bombing Prevention (OBP)	Unclassified	www.dhs.gov/tripwire https://tripwire.dhs.gov

Page intentionally left blank.

Appendix F: Targeted Threat and Security Engagements[71]

Targeted Threat and Security Engagements

As Office of Infrastructure Protection (IP) receives threat information from the Intelligence Community (IC), in coordination with the cross sector councils, IP validates and determines if a security engagement is needed, and to what degree outreach should be conducted to share this information with the appropriate public and private sector critical infrastructure owners and operators. Members of the Critical Infrastructure Cross-Sector Council, the National Council of Information Sharing and Analysis Centers (NCI), the Regional Consortium Coordinating Council (RC3), and the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC) may also request a targeted threat and security engagement to provide or request information on emerging threats and/or issues.

The following key steps will generally occur as part of this process:

- IP and members or member representatives of the Critical Infrastructure Cross-Sector Council, the NCI, the RC3, the Federal Senior Leadership Council (FSLC), and the SLTTGCC are made aware of specific threat information.
  - Potential channels of threat information include Office of Intelligence and Analysis (I&A), Counter Terrorism Advisory Board (CTAB) meetings, the Office of Cyber and Infrastructure Analysis (OCIA), critical infrastructure partners, or other channels.
- The Engagement Working Group (EWG) is convened to discuss the strategy behind targeted threat and security engagements with critical infrastructure partners in the affected sector and/or geographic region.
- The EWG, in coordination with the IP lead, makes a recommendation to the Assistant Secretary (A/S) on the need and appropriate means to conduct targeted engagements.
- IP coordinates the execution of the engagement strategy approved by the A/S and notifies the appropriate public and private sector critical infrastructure partners.
- For classified threat and security information engagements, IP will take two steps:
  - Utilize a range of options, including secure communications capabilities and government liaison officers in stakeholders' operating locations, to share the classified material with cleared recipients in industry and government.
  - Coordinate with I&A to develop For Official Use Only (FOUO) messaging and/or tearline summaries to provide government partners and members of the Cross-Sector Councils with actionable recommendations and key objectives to share with their constituencies. This messaging may be developed within a reasonable period after threat and security engagement meetings.
- Following the engagement, IP will coordinate with the Critical Infrastructure Cross-Sector Council, the NCI, the RC3, the FSLC, the SLTTGCC, and other critical infrastructure

[71] Office of Infrastructure Protection and Cross-Sector Councils, *Coordination Plan for Targeted Threat and Security Engagements*, (February 2016).

partners to discuss whether the information was useful and to identify any best practices or lessons learned from the engagement (to inform future engagements).

Periodic Threat and Security Engagements

On a periodic basis, IP, in coordination with I&A and OCIA, will provide critical infrastructure partners with threat and intelligence information as part of a routine engagement effort to test and maintain communications processes and cross-sector situational awareness.

This recurring activity will include notifications to all relevant partners, a threat and intelligence briefing, discussion, and follow-up to capture lessons learned.

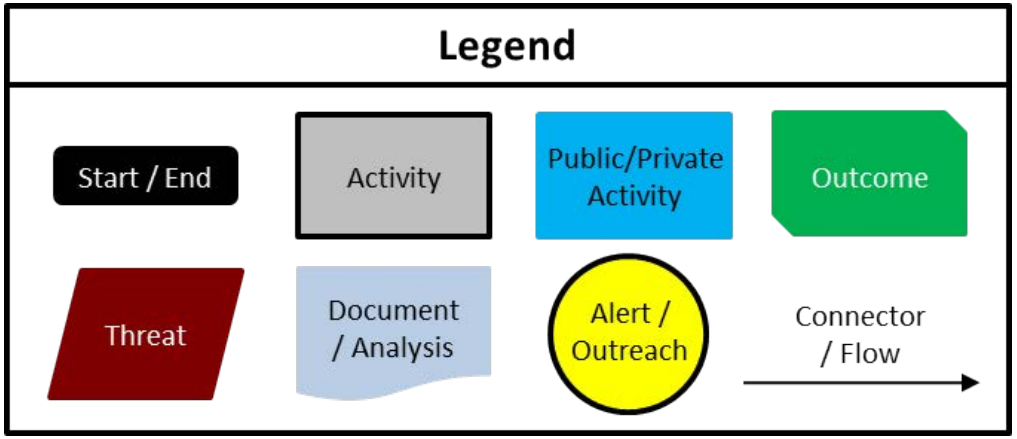
The engagements will provide opportunities for the Federal Government, the Critical Infrastructure Cross-Sector Council, the NCI, the RC3, the SLTTGCC, and other critical infrastructure partners to share information, products, best practices, and collection priorities.

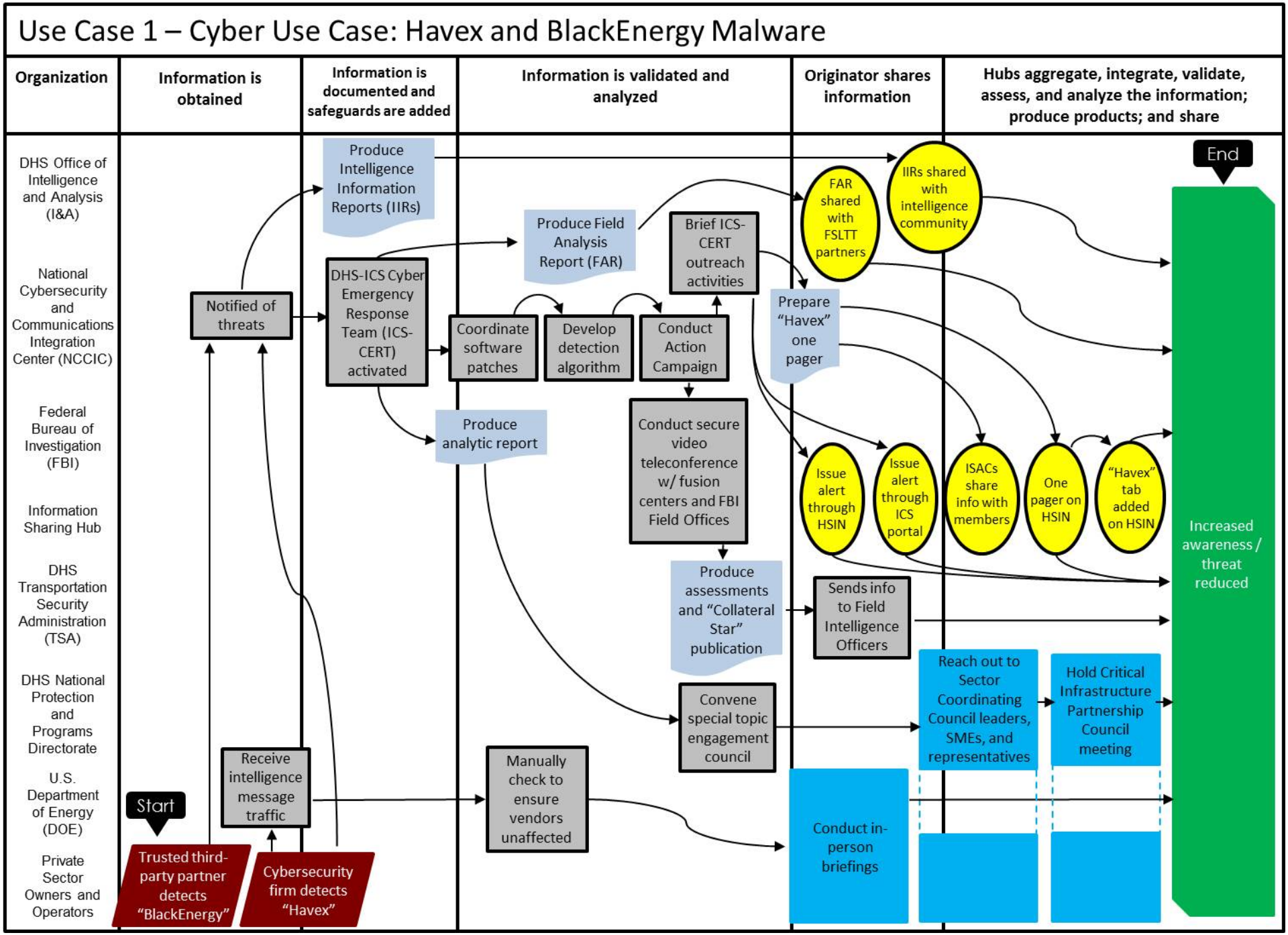
These efforts will provide partners with current and relevant intelligence and threat information and recommended protective measures for reducing risk. IP will coordinate with the Critical Infrastructure Cross-Sector Council, the NCI, the RC3, the FSLC, the SLTTGCC, and other critical infrastructure partners to ensure that the list of appropriately cleared private sector personnel is maintained on a regular basis.

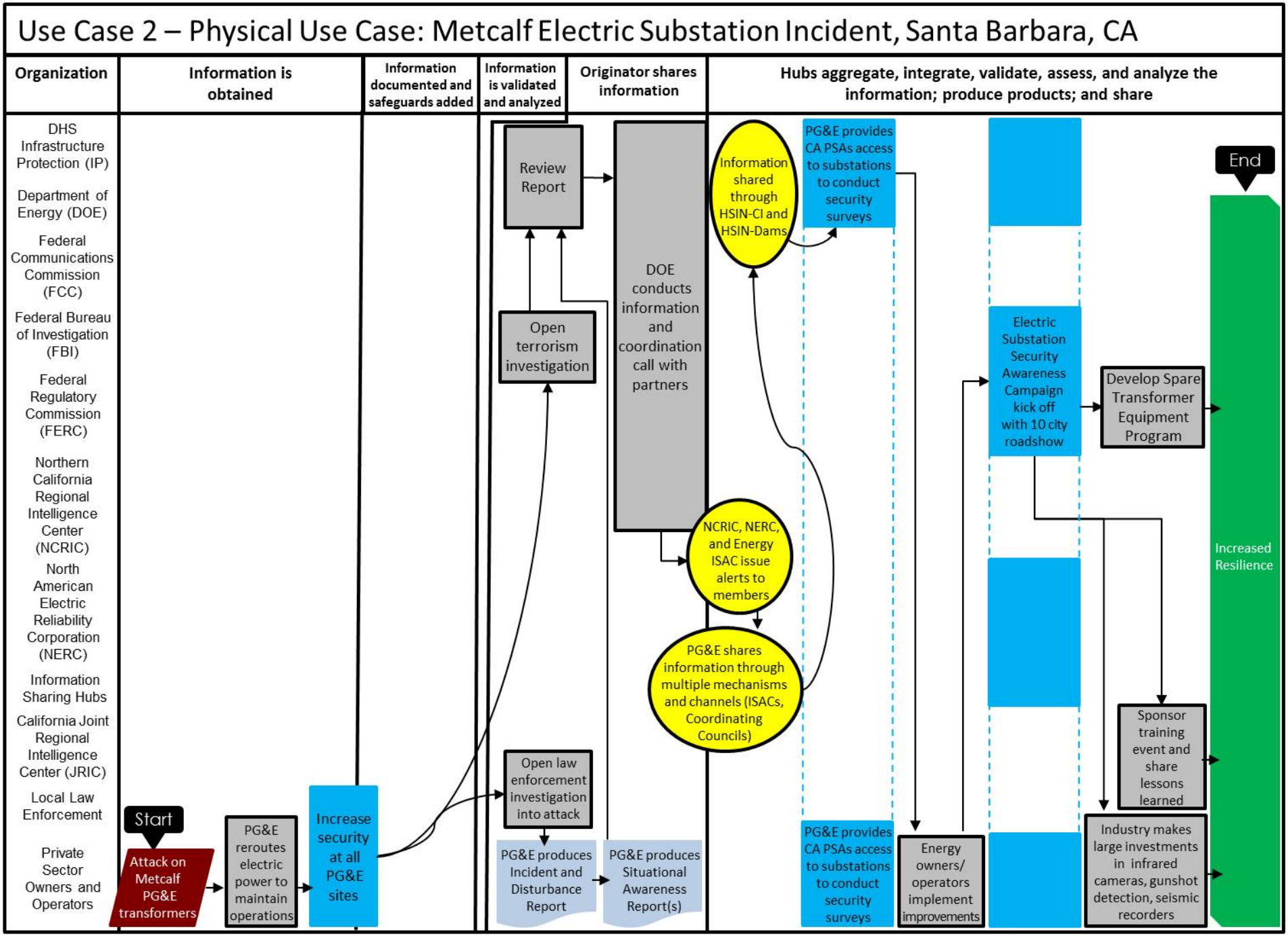
This process will also be used to establish and maintain contacts and relationships with critical infrastructure partners to facilitate the threat and security engagement process under more urgent conditions.

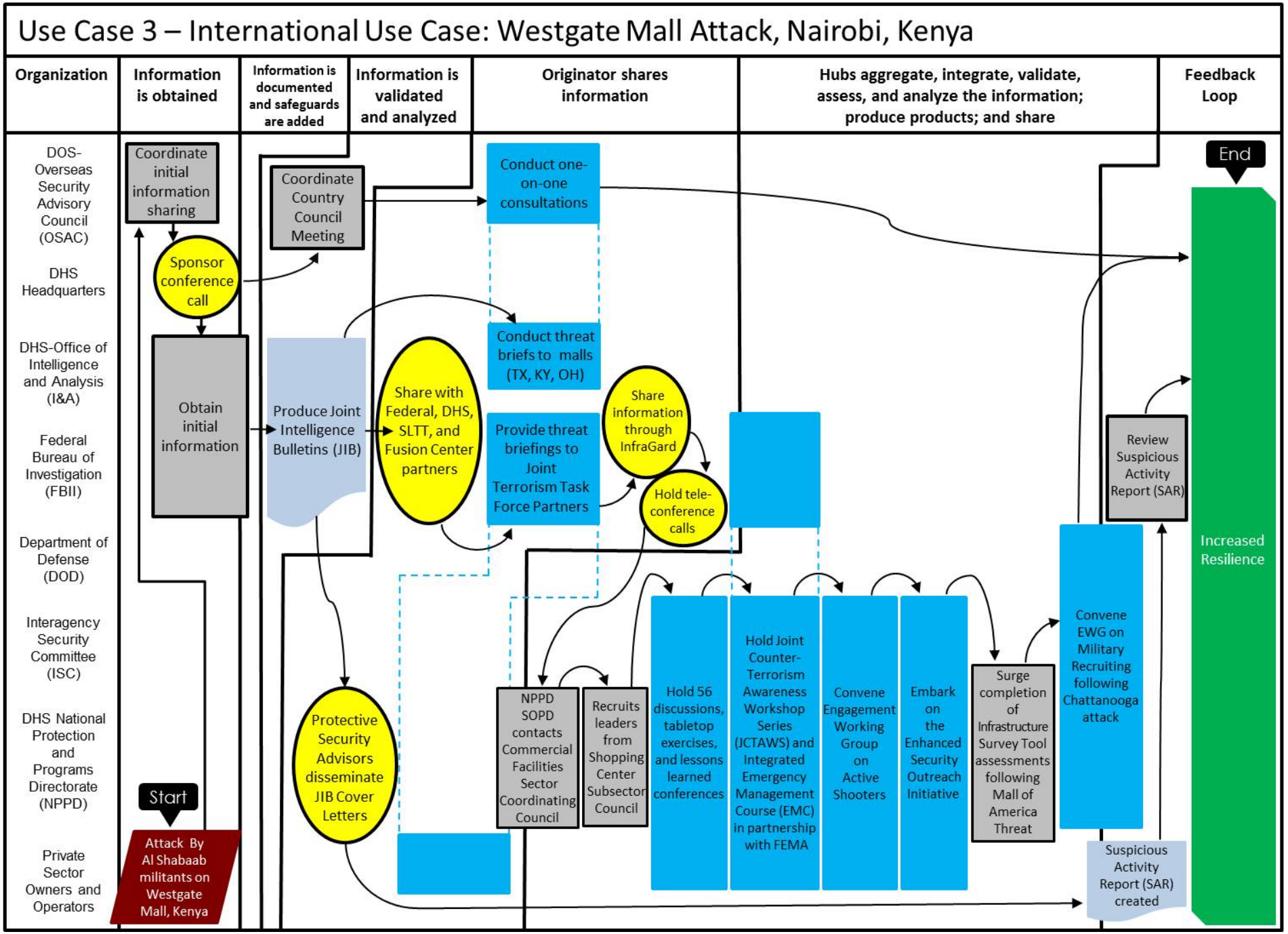
Appendix G: Use Case Information Flow Maps

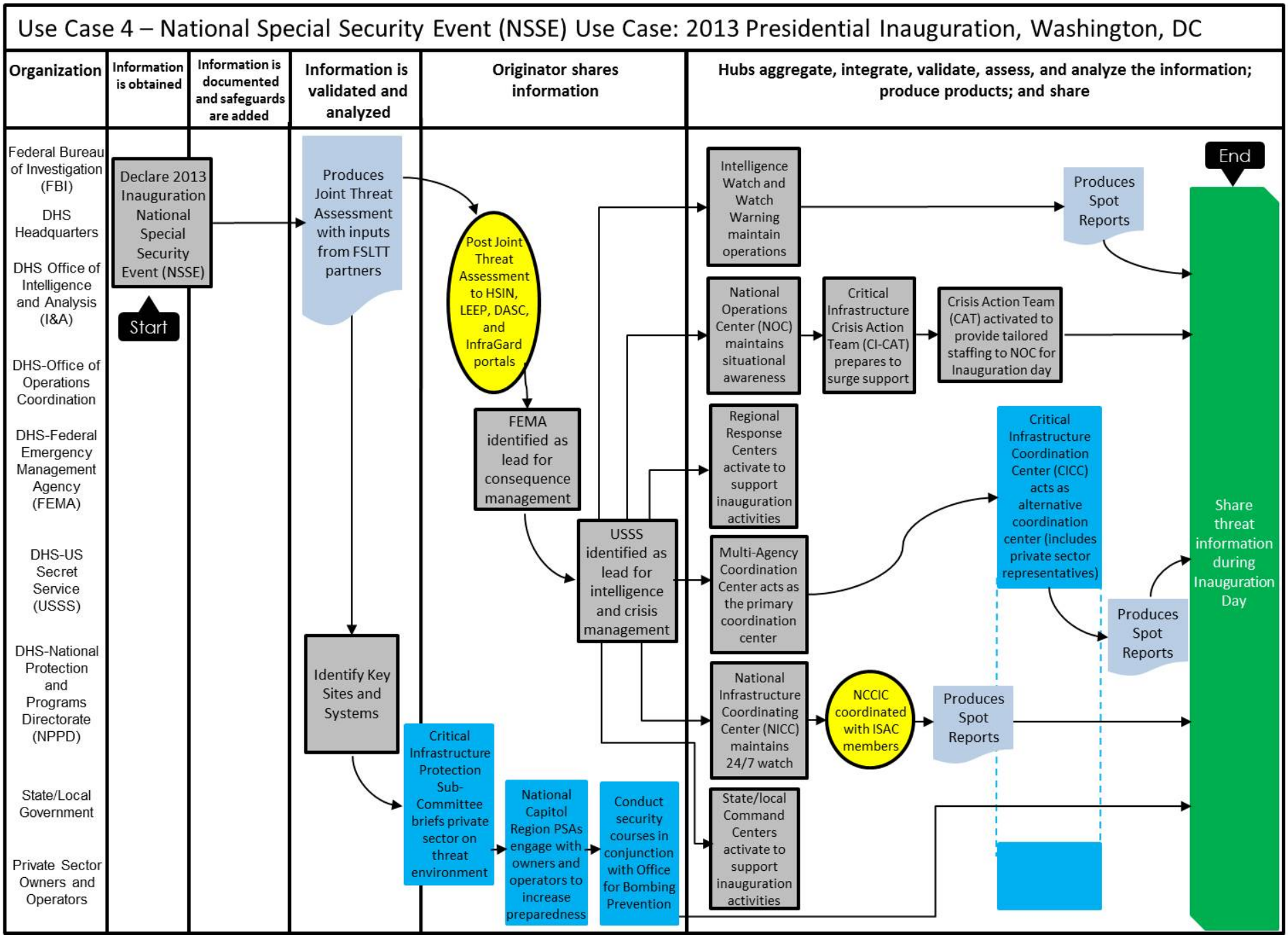
These flow maps provide another, more detailed, visualization of the information flows in each of the use cases from Section 4.




Use Case 1 – Cyber Use Case: Havex and BlackEnergy Malware
Organization
Information is obtained
Information is documented and safeguards are added
Information is validated and analyzed
Originator shares information
Hubs aggregate, integrate, validate, assess, and analyze the information; produce products; and share
DHS Office of Intelligence and Analysis (I&A)
National Cybersecurity and Communications Integration Center (NCCIC)
Federal Bureau of Investigation (FBI)
Information Sharing Hub
DHS Transportation Security Administration (TSA)
DHS National Protection and Programs Directorate
U.S. Department of Energy (DOE)
Private Sector Owners and Operators
Start
Trusted third-party partner detects "BlackEnergy"
Cybersecurity firm detects "Havex"
Notified of threats
Receive intelligence message traffic
Produce Intelligence Information Reports (IIRs)
DHS-ICS Cyber Emergency Response Team (ICS-CERT) activated
Produce Field Analysis Report (FAR)
Coordinate software patches
Develop detection algorithm
Conduct Action Campaign
Brief ICS-CERT outreach activities
Produce analytic report
Conduct secure video teleconference w/ fusion centers and FBI Field Offices
Manually check to ensure vendors unaffected
Produce assessments and "Collateral Star" publication
Convene special topic engagement council
FAR shared with FSLTT partners
IIRs shared with intelligence community
Prepare "Havex" one pager
Issue alert through HSIN
Issue alert through ICS portal
ISACs share info with members
One pager on HSIN
"Havex" tab added on HSIN
Sends info to Field Intelligence Officers
Reach out to Sector Coordinating Council leaders, SMEs, and representatives
Hold Critical Infrastructure Partnership Council meeting
Conduct in-person briefings
End
Increased awareness / threat reduced


Use Case 2 – Physical Use Case: Metcalf Electric Substation Incident, Santa Barbara, CA
Organization
Information is obtained
Information documented and safeguards added
Information is validated and analyzed
Originator shares information
Hubs aggregate, integrate, validate, assess, and analyze the information; produce products; and share
DHS Infrastructure Protection (IP)
Department of Energy (DOE)
Federal Communications Commission (FCC)
Federal Bureau of Investigation (FBI)
Federal Regulatory Commission (FERC)
Northern California Regional Intelligence Center (NCRIC)
North American Electric Reliability Corporation (NERC)
Information Sharing Hubs
California Joint Regional Intelligence Center (JRIC)
Local Law Enforcement
Private Sector Owners and Operators
Start
Attack on Metcalf PG&E transformers
PG&E reroutes electric power to maintain operations
Increase security at all PG&E sites
Review Report
Open terrorism investigation
Open law enforcement investigation into attack
DOE conducts information and coordination call with partners
PG&E produces Incident and Disturbance Report
PG&E produces Situational Awareness Report(s)
Information shared through HSIN-CI and HSIN-Dams
NCRIC, NERC, and Energy ISAC issue alerts to members
PG&E shares information through multiple mechanisms and channels (ISACs, Coordinating Councils)
PG&E provides CA PSAs access to substations to conduct security surveys
PG&E provides CA PSAs access to substations to conduct security surveys
Energy owners/ operators implement improvements
Electric Substation Security Awareness Campaign kick off with 10 city roadshow
Develop Spare Transformer Equipment Program
Sponsor training event and share lessons learned
Industry makes large investments in infrared cameras, gunshot detection, seismic recorders
End
Increased Resilience


Use Case 3 – International Use Case: Westgate Mall Attack, Nairobi, Kenya
Organization
Information is obtained
Information is documented and safeguards are added
Information is validated and analyzed
Originator shares information
Hubs aggregate, integrate, validate, assess, and analyze the information; produce products; and share
Feedback Loop
DOS-Overseas Security Advisory Council (OSAC)
DHS Headquarters
DHS-Office of Intelligence and Analysis (I&A)
Federal Bureau of Investigation (FBII)
Department of Defense (DOD)
Interagency Security Committee (ISC)
DHS National Protection and Programs Directorate (NPPD)
Private Sector Owners and Operators
Coordinate initial information sharing
Sponsor conference call
Coordinate Country Council Meeting
Obtain initial information
Produce Joint Intelligence Bulletins (JIB)
Share with Federal, DHS, SLTT, and Fusion Center partners
Protective Security Advisors disseminate JIB Cover Letters
Conduct one-on-one consultations
Conduct threat briefs to malls (TX, KY, OH)
Provide threat briefings to Joint Terrorism Task Force Partners
Share information through InfraGard
Hold tele-conference calls
NPPD SOPD contacts Commercial Facilities Sector Coordinating Council
Recruits leaders from Shopping Center Subsector Council
Hold 56 discussions, tabletop exercises, and lessons learned conferences
Hold Joint Counter-Terrorism Awareness Workshop Series (JCTAWS) and Integrated Emergency Management Course (EMC) in partnership with FEMA
Convene Engagement Working Group on Active Shooters
Embark on the Enhanced Security Outreach Initiative
Surge completion of Infrastructure Survey Tool assessments following Mall of America Threat
Convene EWG on Military Recruiting following Chattanooga attack
Review Suspicious Activity Report (SAR)
Suspicious Activity Report (SAR) created
Start
Attack By Al Shabaab militants on Westgate Mall, Kenya
End
Increased Resilience


Use Case 4 – National Special Security Event (NSSE) Use Case: 2013 Presidential Inauguration, Washington, DC
Organization
Information is obtained
Information is documented and safeguards are added
Information is validated and analyzed
Originator shares information
Hubs aggregate, integrate, validate, assess, and analyze the information; produce products; and share
Federal Bureau of Investigation (FBI)
DHS Headquarters
DHS Office of Intelligence and Analysis (I&A)
DHS-Office of Operations Coordination
DHS-Federal Emergency Management Agency (FEMA)
DHS-US Secret Service (USSS)
DHS-National Protection and Programs Directorate (NPPD)
State/Local Government
Private Sector Owners and Operators
Declare 2013 Inauguration National Special Security Event (NSSE)
Start
Produces Joint Threat Assessment with inputs from FSLTT partners
Post Joint Threat Assessment to HSIN, LEEP, DASC, and InfraGard portals
FEMA identified as lead for consequence management
USSS identified as lead for intelligence and crisis management
Identify Key Sites and Systems
Critical Infrastructure Protection Sub-Committee briefs private sector on threat environment
National Capitol Region PSAs engage with owners and operators to increase preparedness
Conduct security courses in conjunction with Office for Bombing Prevention
Intelligence Watch and Watch Warning maintain operations
National Operations Center (NOC) maintains situational awareness
Critical Infrastructure Crisis Action Team (CI-CAT) prepares to surge support
Crisis Action Team (CAT) activated to provide tailored staffing to NOC for Inauguration day
Regional Response Centers activate to support inauguration activities
Multi-Agency Coordination Center acts as the primary coordination center
National Infrastructure Coordinating Center (NICC) maintains 24/7 watch
NCCIC coordinated with ISAC members
State/local Command Centers activate to support inauguration activities
Produces Spot Reports
Critical Infrastructure Coordination Center (CICC) acts as alternative coordination center (includes private sector representatives)
Produces Spot Reports
Produces Spot Reports
End
Share threat information during Inauguration Day

Page intentionally left blank.

Page intentionally left blank.

Homeland
Security