**Cross Domain Threat and Risk Information Sharing**

**Scenario Descriptions**

**Table of Contents**

**DRAFT**

Table of Contents

[1. Background 1](#_Toc414269184)

[2. Purpose 1](#_Toc414269185)

[2.1 Communities of Interest 2](#_Toc414269186)

[2.2 Cross Domain Key Communities 2](#_Toc414269187)

[3. Cross Domain Use Cases 3](#_Toc414269188)

[Appendix A— Enhanced Shared Situational Awareness (ESSA) Information Exchanges 23](#_Toc414269189)

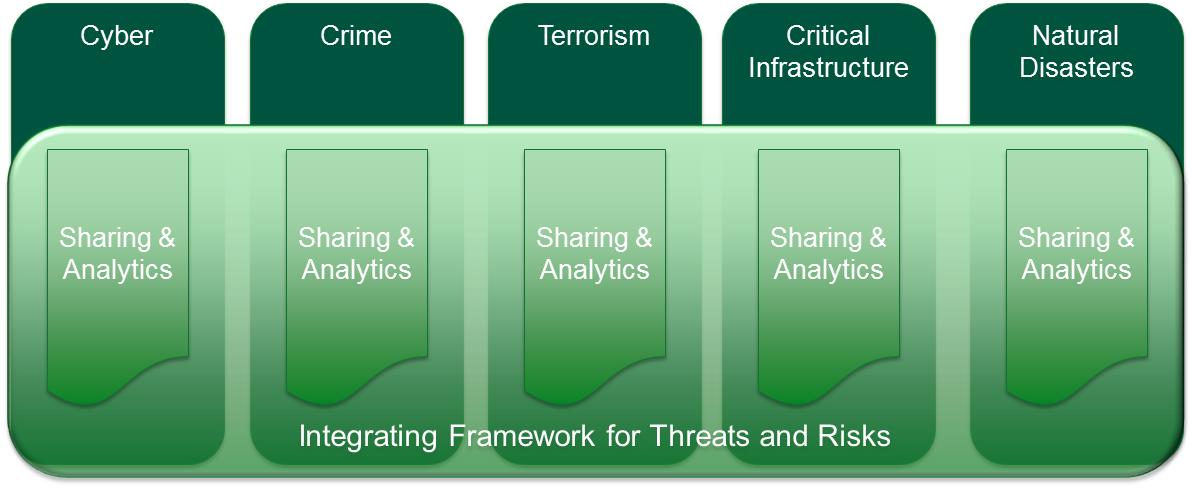
[Appendix B— Document History 24](#_Toc414269190)

[Appendix C—Fusion Center Cyber Information Sharing 25](#_Toc414269191)

[Fusion Center Cross-Domain Sharing 25](#_Toc414269192)

# Background

Threats and risks are increasingly multi-dimensional in nature – spanning physical space and cyber space. Threat actors understand and exploit our government’s stove piped approach to sharing and analyzing information which, leads to ineffective collaboration and mediation. In the broadest sense, organizations manage threats and risks in order to provide a systematic response to uncertainties and enhance situational awareness. Multiple communities have developed data and exchange schema and interfaces for sharing information about threats, risks, and incidents that impact important government, commercial and personal assets and privacy. While each of these schema and interfaces provides value for a specific community it is difficult to federate these multiple representations to arrive at broad-based, planning, simulation, assessment, situational awareness and forensics, and to then enact the appropriate courses of action. Cyber related attacks have added a new dimension that stresses traditional assessment, monitoring and mitigation strategies. Only by federating information across multiple domains (such as cyber, criminal, terrorism, critical infrastructure, intelligence and defense) irrespective of technical and political boundaries, can we effectively counter multi-dimensional intentional threats, natural events and system failures. Refer to the below illustration of a cross-domain integrated framework for threats and risks.

[](http://threatrisk.informationfederation.org/wp/wp-content/uploads/2015/02/ThreatRiskFramework.jpg)

# Purpose

This document is meant to help capture a sampling of scenarios that can potentially be used help fill the gaps in cross domain information sharing requirements, to validate definitions and model structures, and assist in identifying opportunities where an information sharing models may be extended to address needs of a specific community. These cross domain use cases provide the details of the business problem, the stakeholders/actors/partners involved, business process rules, types of information exchanges, detailed data elements and any policy elements associated with access control, PII data, and security classification fabrics.

## Communities of Interest

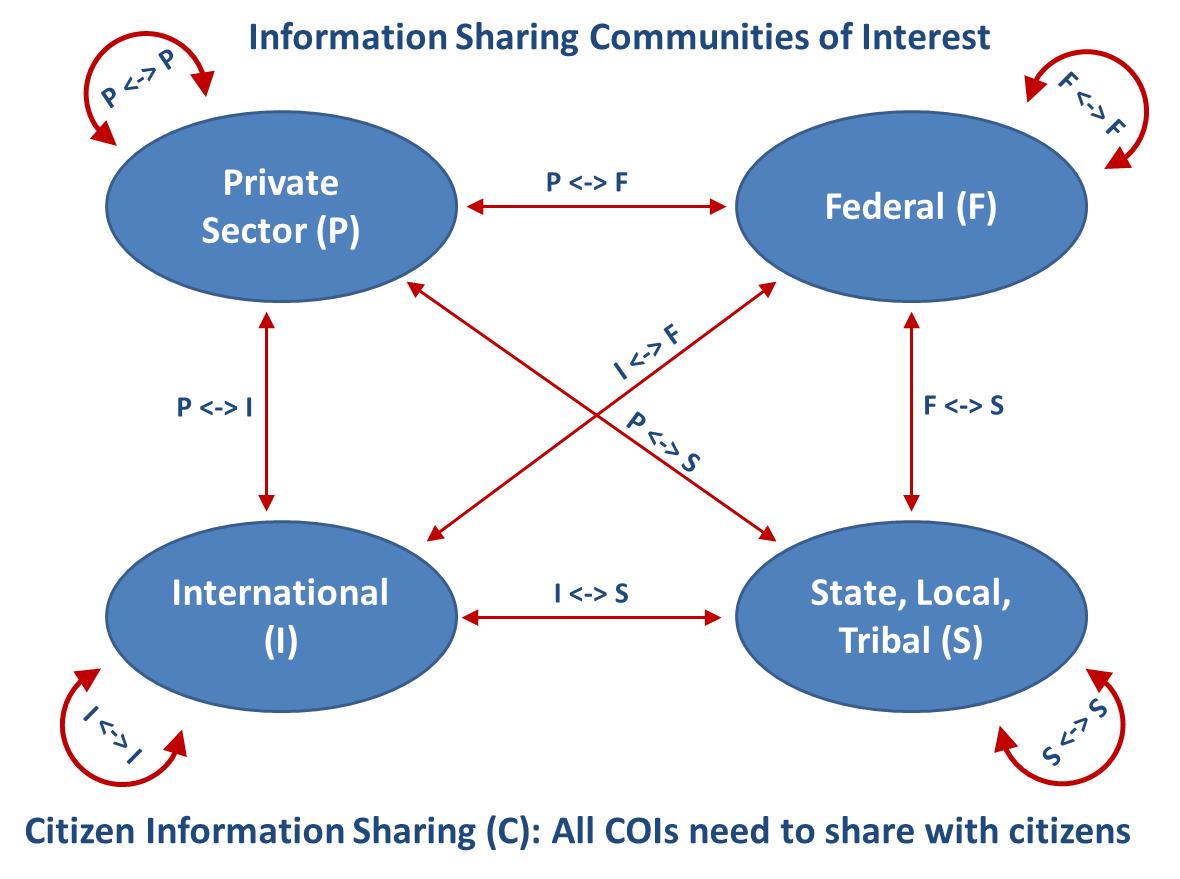
The use cases outlined in this document may be used for identifying and understanding how seemingly different communities can more effectively share threat and risk information to address common concerns. These shared communities are frequently referred to as “Communities of Interest” (COI). The following table describes the different combinations that comprise the cross domain COI, and how these communities may be associated with the specific use cases under consideration in this document.

## Cross Domain Key Communities

There are four key COI identified as potential stakeholders for sharing cross domain threat and risk information:

* Private Sector (P): Private sector corporations including all domestic and international corporations, particularly those most susceptible industries and privately owned and managed critical infrastructure;
* Federal (F): Federal government departments and agencies;
* State, Local, Tribal and Territorial (S): A Non-federal government department and agencies;
* International (I): International government mission partners; and
* Citizens (C): Private Citizens.

The following illustration depicts the aforementioned COIs and their potential paths and opportunities to engage in cross domain threat and risk information sharing. Relevant and responsible sharing of information with private citizen sharing may happen across all the COIs, and are not separately called out in the diagram below.



The following table depicts several combinations for cross domain sharing of threat and risk information among various COI.

|  |  |
| --- | --- |
| Communities | Description |
| P ↔ F | Private Sector to Federal Government |
| P ↔ S | Private Sector to State, Local, Tribal Government |
| P ↔ I | Private Sector to International Government Partners |
| F ↔S | Federal Government to State, Local, Tribal Governments |
| F ↔I | Federal Government to International Government Partners |
| S ↔ I | State, Local, Tribal Government to International Government Partners |
| P ↔P | Within Private Sector |
| F ↔ F | Within Federal Government Agencies |
| S ↔ S | Within State and local agencies (intra and inter) |
| I ↔ I | Among International governments (through bi-lateral or international treaties) |
| F ↔ C | Federal Government sharing with Citizen |
| P ↔ C | Private Sector sharing with Citizen |
| S ↔ C | State Government sharing with Citizen |
| C ↔ C | Citizen sharing with Citizen |

# Cross Domain Use Cases

There are a number of applicable use cases to help identify the need for a cross domain threat and risk information sharing model. Each of these use cases contain information about the potential COIs/partners, business processes, enduring functional exchanges[[1]](#footnote-1), assumptions, and classification fabrics that could be involved/used. These use cases are organized according to the following categories and the following tables lay out potential cross domain threat and risk information sharing scenarios:

* **Integrated Threat Assessment for Critical Infrastructure**: Our national and economic security rest upon a foundation of highly interdependent critical infrastructures and these infrastructures cover a large number of sectors (e.g., financial, energy, transportation, health care) that are inter-dependent and interconnected. Having a holistic and cohesive understanding and analysis of current and potential risks to CIKR is essential to a wide variety of stakeholders.
* **Mission Assurance and Critical Infrastructure Cascading Dependencies**: In the Defense community, significant attention has been devoted to understanding the internal processes and supporting systems that rely on physical infrastructure and key assets. Threats to the maintenance and security of those critical infrastructure support systems can be cyber in nature and can have both kinetic and non-kinetic effects. Mission assurance requires keeping infrastructures, assets, and supply chains robust, resilient, redundant and secure.
* **Integrated Risk Assessment for the Defense Industrial Base (DIB)**: Partnerships between the Defense and Homeland Security communities enables DIB private sector Critical Infrastructure and Key Resource (CIKR) owners and operators to engage in critical infrastructure protection value-added activities with the Federal Government that are important for our nation’s security.
* **Victim Notification**: In the Justice and Public Safety community, significant attention has been devoted to ensure that crime victims and survivors have opportunities to be safely and actively engaged participants in their cases and in the overall justice process. Victims of cyber threats may be categorized as: victim information compromised as part of a cyber-intrusion; victim is directly involved in a cyber-enabled crime
* **Investigatory Referral**: A situation where a two-person police department receives a phone compliant from an elderly couple that they are a victim of fraud via the internet. Since the police department does not have the resources to handle the case in addition to the case not being in its jurisdiction; the case is referred to the local Wells Spring FBI Task Force for review of similar cases and appropriate action. Alternately, the community could also setup thresholds that could automatically trigger/escalate a specific case, or collection to appropriate entities at the local, state, regional or federal levels.
* **Deconfliction of (Cybersecurity Threat) Indicators**: A situation where Police Department A opens a fraud investigation inherited by a fraud compliant of a particular case in City A. Police Department B has a similar case information. Both police departments enter suspected information into the Inter-Crime Complaint Center Platform, at which point both departments deconflict the information and take appropriate action based on information provided in the system. From a cybersecurity perspective, this could also mean deconflicting an IP address/email address that was identified as part of a cybercrime (or pocket litter at a border crossing) with an IP address identified as part of a cyber-intrusion.

## Scenario Story #1

In the early morning of April 16, 2013, the Metcalf, California transmission substation in Silicon Valley was attacked by what federal investigators believe was a highly professional terrorist team. That sniper assault caused 17 transformers to crash severing power to Internet Service Providers and other power users in Silicon Valley. Pacific Gas and Electric (PG&E) was forced to increase and reroute power to the area served by the disabled transmission station. The recovery took 27 days for PG&E to repair and bring the transmission substation back on line.

|  |  |  |
| --- | --- | --- |
| Use Case #1 | | |
| Title | Physical attack on Transformer Yields Cyber and Kinetic Effects | |
| Category | Integrated Threat Assessment for Critical Infrastructure | |
| Domain | * Cybersecurity * Physical Infrastructure Protection | |
| Security Fabric  (e.g., U, LES, S, TS) | U, LES | |
| Scenario Description | PG&E and the Metcalf sniper attack on high-power SCADA-controlled transformers serving Silicon Valley, California | |
| COIs | * Private↔State * State↔Federal * Federal↔Private * State↔Federal * State↔Citizen | |
| Key Stakeholders | | |
| Partners | National Fusion Center Association, Private Sector CI/KR, ISACs, ISAOs, FBI, DHS, Federal Communications Commission, DOE/Office of Electricity Intelligence | |
| Producers | Private Sector CI/KR, ISACs, ISAOs, FBI, DHS | |
| Consumers | National Fusion Center Association, Private Sector CI/KR, ISACs, ISAOs, FBI, DHS, Federal Communications Commission, DOE/Office of Electricity Intelligence | |
| Scenario Details | | |
| Assumptions | Use of NIEM, use of STIX, Emergency Management Messaging and Standards | |
| Exchange Scenario | At 12:58 a.m., AT&T fiber-optic telecommunications cables were cut—in a way that made them hard to repair—in an underground vault near the substation, not far from U.S. Highway 101 just outside south San Jose. It would have taken more than one person to lift the metal vault cover, said people who visited the site.  Nine minutes later, some customers of Level 3 Communications, an Internet service provider, lost service. Cables in its vault near the Metcalf substation were also cut.  At 1:31 a.m., a surveillance camera pointed along a chain-link fence around the substation recorded a streak of light that investigators from the Santa Clara County Sheriff’s office think was a signal from a waved flashlight. It was followed by the muzzle flash of rifles and sparks from bullets hitting the fence.  The substation’s cameras weren’t aimed outside its perimeter, where the attackers were. The shooters appear to have aimed at the transformers’ oil-filled cooling systems. These began to bleed oil, but didn’t explode, as the transformers probably would have done if hit in other areas.  About six minutes after the shooting started, PG&E confirms, it got an alarm from motion sensors at the substation, possibly from bullets grazing the fence, which is shown on video.  Four minutes later, at 1:41 a.m., the sheriff’s department received a 911 call about gunfire, sent by an engineer at a nearby power plant that still had phone service.  Riddled with bullet holes, the transformers leaked 52,000 gallons of oil, then overheated. The first bank of them crashed at 1:45 a.m., at which time PG&E’s control center about 90 miles north received an equipment-failure alarm.  Five minutes later, another apparent flashlight signal, caught on film, marked the end of the attack. More than 100 shell casings of the sort ejected by AK-47s were later found at the site.  At 1:51 a.m., law-enforcement officers arrived, but found everything quiet. Unable to get past the locked fence and seeing nothing suspicious, they left.  A PG&E worker, awakened by the utility’s control center at 2:03 a.m., arrived at 3:15 a.m. to survey the damage. | |
| Business Rules | TBD with stakeholders | |
| Mapping to ESSA’s Enduring Functional Exchanges (EFE) | (1) Configuration/Anomaly Reporting; (2) Knowledge of Threat Actors; (3) Incident Awareness; (4) Indicators and Warnings; (5) Vulnerability Knowledge; (6) Mitigation Strategies; (7) Mitigation Actions & Responses | |
| Data Elements | | |
| Action | Data Elements | Definitions |
|  |  |  |
| Additional Information: | | |

## Scenario Story #2

A sighting from a BioWatch detection system detects the presence of a pathogen or multiple pathogens in a particular location at a particular time that indicates the possibility of a terrorist attack, accidental release of pathogens or natural outbreak. The detection systems report pathogens based on the concentration of the DNA for a pathogen which is rated as low, medium or high. The BioWatch detectors can also provide information about location of the event (indoor vs outdoor) and potentially any geographical patterns. The intelligence community releases notices of suspected terrorist activity from multiple sources, including the monitoring of social media and other classified sources. Such activity is an indicator of an ongoing or possible future attack. The potential Harm from such a bioterrorism attack is significant and includes: potential for significant life loss (approximately 10M plus people would need to be treated if all of LA County is affected), however it is not clear that this was an actual attack and or if people will become infected. If people are going to get infected they must be treated with antibiotics in order to recover. Potential for economic impact and loss of life; potential biohazard issue – contaminated environment; and more.

|  |  |  |
| --- | --- | --- |
| Use Case #2 | | |
| Title | Bio Surveillance Coordination | |
| Category | Integrated Threat Assessment for Critical Infrastructure | |
| Domain | * Public Health Data * Intelligence Information Sharing | |
| Security Fabric  (e.g., U, LES, S, TS) | U, S, TS | |
| Scenario Description | Bio surveillance and Emergency Management “BioWatch” coordination health/chemical related threats with Public Safety, Intelligence Community, and Healthcare providers | |
| COIs | * Private↔State * State↔Federal * Federal↔Private * State↔Citizen | |
| Key Stakeholders | | |
| Partners | local public health officials; local emergency managers (Cal OES); local department of food and agriculture; local fusion center representative; FBI-WMD coordinator; and potentially others who are members of the BioWatch advisory committee | |
| Producers | FBI, HHS, IC, NNFC, Governor’s Office, DHS, International Partners | |
| Consumers | FBI, HHS, IC, NNFC, Governor’s Office, DHS, International Partners | |
| Scenario Details | | |
| Assumptions | Use of NIEM, EDXL | |
| Exchange Scenario | A sighting from a BioWatch detection system detects the presence of a pathogen or multiple pathogens in a particular location at a particular time that indicates the possibility of a terrorist attack, accidental release of pathogens or natural outbreak. The detection systems report pathogens based on the concentration of the DNA for a pathogen which is rated as low, medium or high. The BioWatch detectors can also provide information about location of the event (indoor vs outdoor) and potentially any geographical patterns. The intelligence community releases notices of suspected terrorist activity from multiple sources, including the monitoring of social media and other classified sources. Such activity is an indicator of an ongoing or possible future attack. The potential Harm from such a bioterrorism attack is significant and includes: potential for significant life loss (approximately 10M plus people would need to be treated if all of LA County is affected), however it is not clear that this was an actual attack and or if people will become infected. If people are going to get infected they must be treated with antibiotics in order to recover. Potential for economic impact and loss of life; potential biohazard issue – contaminated environment; and more. | |
| Business Rules | TBD by stakeholders | |
| Mapping to ESSA’s Enduring Functional Exchanges (EFE) | Not Applicable | |
| Data Elements | | |
| Action | Data Elements | Definitions |
|  |  |  |
| Additional Information: | | |

## Scenario Story #3

Recent global survey by Symantec: Half of employees who left or lost their jobs in the last 12 months kept confidential corporate data; 40% plan to use it at their new job:

* Head of an engineering department allegedly was recruited to leave and join another company, and to take trade secrets with him, causing losses of more than $800 million.
* Former network engineer sentenced to 4 years in prison and more than $500,000 in restitution for sabotaging his company’s systems and disrupting operations for more than a month
* Former programmer sabotaged his company’s systems using credentials he harvested before his resignation
* Engineer charged with stealing more than 2 million files containing trade secrets and sending them to his wife outside the country

|  |  |  |
| --- | --- | --- |
| Use Case #3 | | |
| Title | Multi-National Company | |
| Category | Mission Assurance and Critical Infrastructure Cascading Dependencies | |
| Domain | Insider Threat and impact on large multi-national company | |
| Security Fabric  (e.g., U, LES, S, TS) | U | |
| Scenario Description | A variety of potential attack scenarios can be played out against the company, including external and internal attacks. While there is a reasonable security program in place, the company is not able to ensure full in-depth security across all systems and assets | |
| COIs | * Private↔State * State↔Federal * Federal↔Private * State↔Citizen | |
| Key Stakeholders | | |
| Partners | Company Employees, shareholders, customers, government and industry | |
| Producers | Company Employees | |
| Consumers | Shareholders, customer, government | |
| Scenario Details | | |
| Assumptions | Use of NIEM, EDXL | |
| Exchange Scenario | Many scenarios are triggered for considerations of financial gain, reputation damage, stock market manipulation, corporate asset theft, hostile recruitment of key employees. These include:   * Identity Theft: The attacker attacks the end user systems or the corporate assets (cyber or traditional information assets) to obtain the identities of primarily the end users. Subsequently the attackers use these identities to create new credit accounts or access existing assets owned by the victims. * Financial Data Theft: The attackers obtain sensitive financial information about end-users or other entities from corporate assets. These types of information may include credit card data. This information is used to extract money from the affected financial accounts. * Extortion: The attacker obtains the ability to negatively affect corporate assets (e.g. through denial, destruction, disruption, degradation, distortion, data exfiltration, etc.) and blackmail the company. The company pays a ransom to avoid negative consequences. * Money/Financial Instrument Theft: This is traditional direct theft of money (cash or cash-like instruments), or similar financial instruments that can immediately be sold. Both criminals as well as Insiders follow this strategy. This strategy may involve physical and/or cyber theft of money. * Credit Card Data Theft: The attacker targets specifically credit card data and publish it subsequently. This is intended to specifically attack the company’s credibility as a trustworthy merchant. It may result in additional fines, or even in losing the ability to process credit cards in the future. * Internal Corporate Financial Data Theft: By stealing and publishing the company’s internal financial data, the attackers succeed in making internal sales and profit data public. Such data may be a surprise for markets and negatively affect investor sentiment. In addition it may result in regulatory actions against the company * Disable, Destroy, Deny, Degrade, Disrupt Critical Assets: The attacker targets company critical assets and attempts to disable, destroy, deny, degrade, or disrupt (5-Ds) them. This may have a number of reasons:   + Disturb the use of critical assets and negatively influence the ability to operate, cause distraction with employees, customers, and partners   + Inflict damage on the company’s ability to deliver core services specifically to customers (but also employees or partners) * Stock Market Manipulation * Publication of Internal Financial Data: Publication of internal financial data may expose internal deviations from market expectations (both positive and negative). If this happens at critical times, the stock price of the company may fluctuate significantly. This may result in special investment opportunities for the hostile investor, or create market benefits for competitors. * Corporate Asset Theft * Corporate Secret Theft: This is the case of corporate or industrial espionage. Any of the attackers are interested in stealing corporate secrets and other proprietary information. The rationale behind this may be different for each actor:   + The Nation State tries to obtain this data to improve the competitiveness of their own industries   + The Criminal sees an opportunity to monetize this theft in different ways   + The Hostile Investor gains an advantage by better understanding the company’s strengths and weakness with respect to the larger markets they operate in   + The Competitor can leverage the data directly to improve their own products or strategies * Physical Asset Theft: This is case of traditional theft of corporate resource. Typical attackers are criminals that try to enter company facilities and steal equipment, resources, or money. Malicious insiders are also main attackers, since they have very broad opportunities to steal from the company. * Hostile Recruitment of Key Employees: The Competitor tries to hire key employees from the company to improve their own talent base and/or to diminish the talent base of the company. In doing so, the Competitor may also steal Corporate Secrets to identify key employees, better understand their contributions, and learn about their compensation packages. | |
| Business Rules | TBD by stakeholders | |
| Mapping to ESSA’s Enduring Functional Exchanges (EFE) | Not Applicable | |
| Data Elements | | |
| Action | Data Elements | Definitions |
|  |  |  |
| Additional Information: | | |

## Scenario Story #4

In January 2015 Massachusetts has been facing the Hazard of major winter storms across the region. Potential Harm from blizzards and winter storms includes negative economic impact, limited road accessibility, restricted emergency management, non-availability of utility, property damage, personal injury and death, and more. Important Actors include: State Governor, Massachusetts Emergency Management Agency (MEMA), Federal Emergency Management (FEMA), local and state highway departments, fire and local & state police departments, National Guard, neighboring state agencies, residents, etc.

The onset of a winter storm or blizzard may be a undesirable Potential Situation predicted by the National Weather Service (NWS). The Risk of a bad winter storm is determined by the likelihood of occurring, and the potential Harm it can cause to the people and their personal effects (Assets).

|  |  |  |
| --- | --- | --- |
| Use Case #4 | | |
| Title | Natural Disaster | |
| Category | Integrated Threat Assessment for Critical Infrastructure | |
| Domain | Natural Disaster and CIKR | |
| Security Fabric  (e.g., U, LES, S, TS) | U | |
| Scenario Description | A variety of potential attack scenarios can be played out against the company, including external and internal attacks. While there is a reasonable security program in place, the company is not able to ensure full in-depth security across all systems and assets | |
| COIs | * Private↔State * State↔Federal * Federal↔Private * State↔Citizen | |
| Key Stakeholders | | |
| Partners | local transportation officials; local emergency managers; local department of food and agriculture; local fusion center representative; FBI coordinator; health and human services, public works departments, local law enforcement | |
| Producers | FBI, HHS, IC, NNFC, Governor’s Office, DHS, International Partners | |
| Consumers | FBI, HHS, IC, NNFC, Governor’s Office, DHS, International Partners | |
| Scenario Details | | |
| Assumptions | Information Transformation of NIEM, and EDXL | |
| Exchange Scenario | In January 2015 Massachusetts has been facing the Hazard of major winter storms across the region. Potential Harm from blizzards and winter storms includes negative economic impact, limited road accessibility, restricted emergency management, non-availability of utility, property damage, personal injury and death, and more. Important Actors include: State Governor, Massachusetts Emergency Management Agency (MEMA), Federal Emergency Management (FEMA), local and state highway departments, fire and local & state police departments, National Guard, neighboring state agencies, residents, etc.  The onset of a winter storm or blizzard may be a undesirable Potential Situation predicted by the National Weather Service (NWS). The Risk of a bad winter storm is determined by the likelihood of occurring, and the potential Harm it can cause to the people and their personal effects (Assets).  Risk Treatment Strategies at the government level may include:  (i) Closing of government services (avoidance)  (ii) Activation of snow removal services (impact mitigation)  (iii) Coordination with energy utilities and other critical infrastructure provider to prepare for damage (impact mitigation)  (iv) Issuance of special orders (curfew/travel ban, airport shutdown, limited public transport, etc.) (avoidance)  (v) Nothing (acceptance)  Private parties may prepare by:  (i) Contracting of snow removal services (impact mitigation)  (ii) Snow damage insurance (transfer)  (iii) Nothing (acceptance)  After the storm, response Capabilities of MEMA and other state and local emergency responders are determined by available Resources. In severe cases, the Governor may act as Facilitator and issue a State of Emergency declaration (Alter Capabilities Act) to improve local and state emergency response Capabilities. | |
| Business Rules | TBD by stakeholders | |
| Mapping to ESSA’s Enduring Functional Exchanges (EFE) | Not Applicable | |
| Data Elements | | |
| Action | Data Elements | Definitions |
|  |  |  |
| Additional Information: | | |

## Scenario Story #5

Realtor Compromise: A local realtor’s database of clients and upcoming sales was compromised through a spear phishing attack. On the day of several closings, emails were sent to the realtors representing the buying parties that appeared to coming from the seller’s realtor. These emails stated that the seller would prefer all the proceeds be wired to a specific account instead of using a cashier’s check. On several occasions, realtors wired the proceeds and lost several hundred thousand dollars.

|  |  |  |
| --- | --- | --- |
| Use Case #5 | | |
| Title | Personal Financial Data Compromise through Spear Phishing | |
| Category | Integrated Threat Assessment for Critical Infrastructure | |
| Domain | * Financial * Real Estate Sector | |
| Security Fabric  (e.g., U, LES, S, TS) | U, LES | |
| Scenario Description | Electronic Financial PII compromised through spear phishing attack | |
| COIs | * Citizen↔State * Private↔State * State↔Federal * Federal↔Private * State↔Citizen | |
| Key Stakeholders | | |
| Partners | ISAC, ISAO, NNFC, FBI, DHS | |
| Producers | ISAC, ISAO, DHS, FBI | |
| Consumers | ISAC, ISAO, NNFC, FBI, DHS | |
| Scenario Details | | |
| Assumptions | Information Transformation of STIX to NIEM | |
| Exchange Scenario | On the day of several closings, emails were sent to the realtors representing the buying parties that appeared to coming from the seller’s realtor. These emails stated that the seller would prefer all the proceeds be wired to a specific account instead of using a cashier’s check. On several occasions, realtors wired the proceeds and lost several hundred thousand dollars. | |
| Business Rules | TBD by stakeholders | |
| Mapping to ESSA’s Enduring Functional Exchanges (EFE) | (1) Configuration/Anomaly Reporting; (2) Knowledge of Threat Actors; (3) Incident Awareness; (4) Indicators and Warnings; (5) Vulnerability Knowledge; (6) Mitigation Strategies; (7) Mitigation Actions & Responses | |
| Data Elements | | |
| Action | Data Elements | Definitions |
|  |  |  |
| Additional Information: | | |

## Scenario Story #5

Narrative

|  |  |  |
| --- | --- | --- |
| Use Case #5 | | |
| Title | Intellectual Property and Foreign Policy Crisis | |
| Category | Integrated Threat Assessment for Critical Infrastructure | |
| Domain | * Retail * Financial (Public and Private Sector Networks) | |
| Security Fabric  (e.g., U, LES, S, TS) | XXX | |
| Scenario Description | Intellectual property compromise leads to a foreign policy crisis | |
| COIs | * XX * XX | |
| Key Stakeholders | | |
| Partners | XXX | |
| Producers | XXX | |
| Consumers | XXX | |
| Scenario Details | | |
| Assumptions |  | |
| Exchange Scenario | Detailed description of how the scenario would “play out” in 3-4 bullets. | |
| Business Rules |  | |
| Mapping to ESSA’s Enduring Functional Exchanges (EFE) | Refer to the ESSA identified Enduring Functional Exchanges [(1) Configuration/Anomaly Reporting; (2) Knowledge of Threat Actors; (3) Incident Awareness; (4) Indicators and Warnings; (5) Vulnerability Knowledge; (6) Mitigation Strategies; (7) Mitigation Actions & Responses]. Determine which EFE’s (1 thru 7) might be used during the scenario based upon the scenario’s participants. Each participant’s mission-specific operations will guide how many, and how much of each functions they are able to perform. | |
| Data Elements | | |
| Action | Data Elements | Definitions |
|  |  |  |
| Additional Information: | | |

## Scenario Story #7

PBX Compromise: A local hotel’s private branch exchange (PBX), a telephone switching system, was compromised. The PBX ran an old version of SSH (secure shell) and was compromised using a well-known exploit and was launched from a foreign adversary. Once compromised the PBX was reprogrammed to continuously dial 911. The result of this compromise was a telephony denial of service (TDoS) against the local 911 call center that ran for approximately 12 hours.

|  |  |  |
| --- | --- | --- |
| Use Case #7 | | |
| Title | Foreign Syndicate Attacks Hotel | |
| Category | Integrated Threat Assessment for Critical Infrastructure | |
| Domain | * Retail Industry * Critical Infrastructure, Public Safety | |
| Security Fabric  (e.g., U, LES, S, TS) | U, LES | |
| Scenario Description | TDoS infiltration of hotel’s telephone system by organized syndicate degrades public confidence in critical safety infrastructure. | |
| COIs | * Private↔State * State↔Federal * Federal↔Private | |
| Key Stakeholders | | |
| Partners | National Retail Federation, SLTT, Fusion Center, FBI, DHS, ISAC, ISAO | |
| Producers | FBI, DHS, ISAC, ISAO, Fusion Center | |
| Consumers | National Retail Federation, SLTT, Fusion Center, FBI, DHS, ISAC, ISAO | |
| Scenario Details | | |
| Assumptions | Proprietary IT monitoring system (e.g., IDS), Information Transformation of STIX to NIEM | |
| Exchange Scenario | A local hotel’s private branch exchange (PBX), a telephone switching system, was compromised. The PBX ran an old version of SSH (secure shell) and was compromised using a well-known exploit and was launched from a foreign adversary. Once compromised the PBX was reprogrammed to continuously dial 911. The result of this compromise was a telephony denial of service (TDoS) against the local 911 call center that ran for approximately 12 hours. | |
| Business Rules | TBD by Stakeholders | |
| Mapping to ESSA’s Enduring Functional Exchanges (EFE) | (1) Configuration/Anomaly Reporting; (2) Knowledge of Threat Actors; (3) Incident Awareness; (4) Indicators and Warnings; (5) Vulnerability Knowledge; (6) Mitigation Strategies; (7) Mitigation Actions & Responses | |
| Data Elements | | |
| Action | Data Elements | Definitions |
|  |  |  |
| Additional Information: | | |

## Scenario Story #8

Narrative

|  |  |  |
| --- | --- | --- |
| Use Case #8 | | |
| Title | DoD Information Sharing Portal | |
| Category | Mission Assurance and Critical Infrastructure Cascading Dependencies | |
| Domain | * Critical Infrastructure (CONUS) * Cybersecurity (particularly, Military Installations and Fusion Centers) | |
| Security Fabric  (e.g., U, LES, S, TS) | S, TS | |
| Scenario Description | Defense Critical Infrastructure Intelligence Network (DCIIN) DoD portal that provides information and intelligence related to DoD critical infrastructure assets for use by SLTTs, USG, and the IC. The need for timely cross domain dissemination between JWICS SharePoint instances (which it currently exists) to other systems and servers on other classification domains is an important step for improved information sharing, accessibility and direct support. | |
| COIs | * Federal↔Federal * Federal↔State | |
| Key Stakeholders | | |
| Partners | 1. Department of Defense 2. Homeland Security 3. Intelligence 4. Critical Infrastructure 5. Fusion Centers   Local Law Enforcement   1. Emergency Management | |
| Producers | DoD | |
| Consumers | SLTT, Fusion Centers, USG/IC | |
| Scenario Details | | |
| Assumptions | Information Transformation of STIX to NIEM and other Proprietary schemas and languages. | |
| Exchange Scenario | DCIIN includes ArcGIS mapping, intelligence reporting, and key workspaces for daily Defense Critical Infrastructure staff functions. As the user set for this data expands, the need for timely cross domain dissemination between JWICS SharePoint instances (which it currently exists) to other systems and servers on other classification domains is an important step for improved information sharing, accessibility and direct support to Services, Combatant Commands and the war fighter. Currently, this information is not assessable to those who need it most - those serving at CONUS installations and state fusion centers. | |
| Business Rules | TBD by stakeholders | |
| Mapping to ESSA’s Enduring Functional Exchanges (EFE) | (1) Configuration/Anomaly Reporting; (2) Knowledge of Threat Actors; (3) Incident Awareness; (4) Indicators and Warnings; (5) Vulnerability Knowledge; (6) Mitigation Strategies; (7) Mitigation Actions & Responses | |
| Data Elements | | |
| Action | Data Elements | Definitions |
|  |  |  |
| Additional Information: | | |

## Scenario Story #9

Due to the classified and sensitive nature of a potential insider threat to a DOD facility or infrastructure, the follow compelling cross-domain scenario is for illustrative purposes only: On March 18, 2014 IRS, Pennsylvania reported that a former employee took home a computer thumb drive that contained personal information on 20,000 current and former employees and contractors. The information included Social Security numbers, names and addresses. The thumb drive was plugged into the employee’s unsecured network, which could have left the information vulnerable.

According to the US DHS – CERT, an insider threat is generally defined as a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally misused that access to negatively affect the confidentiality, integrity, or availability of the organization's information or information systems. Other US government organizations like Defense Security Services have very similar definitions. The key message is the ability for a trusted resource to intentionally (or unintentionally) take actions (but are not limited to, espionage, unauthorized disclosure of information, etc.) that are detrimental to an organizations’ operational viability. This type of threat is not limited to government only, and is pervasive across all types of organizations. What leads to Insider Threat incidents: Some reasons include: Need or desire for money; Conflicting ideologies or disaffected political sympathies; and Psychological factors (e.g., exaggerated desire for adventure/excitement, ego gratification, misplaced anger, etc.).

Key Indicators: Not every person who exhibits one or more of these indicators is involved with illicit behavior, but most of the persons who have been involved with espionage were later found to have displayed one or more of these indicators.

• Failure to report overseas travel or contact with foreign nationals

• Seeking to gain higher clearance or expand access outside the job scope

• Engaging in classified conversations without a need to know

• Working hours inconsistent with job assignment or insistence on working in private

• Exploitable behavior traits

• Repeated security violations

• Attempting to enter areas not granted access to

|  |  |  |
| --- | --- | --- |
| Use Case #9 | | |
| Title | DoD Information Sharing Portal | |
| Category | Integrated Risk Assessment for the Defense Industrial Base (DIB) | |
| Domain | * Critical Infrastructure (Defense Manufacturing Sector; R&D Facilities) * Cybersecurity (Insider Threat, Espionage, Sabotage) | |
| Security Fabric  (e.g., U, LES, S, TS) | S, TS | |
| Scenario Description | Defense Security Services (DSS) interest in using the Threat and Risk Model to automate machine-to-machine information sharing along with the establishment of a normalized language/date dictionary, automated system for ingest of 34,000+ incident reports. Model and ontology will allow for an increase of time spent on analysis and the ability to streamline information sharing of potential physical and cyber threats to national security with other DoD and DSS stakeholders. | |
| COIs | * Federal↔Federal * Federal↔State * Federal↔Private * Federal↔Citizen | |
| Key Stakeholders | | |
| Partners | * DSS * Object Management Group (OMG) * 40+ DoD Components * 28 Federal D/As * LE and Counterintelligence (CI) Agencies * Cleared Industrial Contractors | |
| Producers | DoD | |
| Consumers | USG, SLTTs, CIKR owners and operators | |
| Scenario Details | | |
| Assumptions | Use of NIEM, use of STIX | |
| Exchange Scenario | * Company A reports a security violation where removable media was introduced in a SCIF computer * 5000+ documents were copied onto this removable media * Information included classified plans for NATO troop deployments in Easter Europe | |
| Business Rules |  | |
| Mapping to ESSA’s Enduring Functional Exchanges (EFE) | 1) Configuration/Anomaly Reporting; (2) Knowledge of Threat Actors; (3) Incident Awareness; (4) Indicators and Warnings; (5) Vulnerability Knowledge; (6) Mitigation Strategies; (7) Mitigation Actions & Responses | |
| Data Elements | | |
| Action | Data Elements | Definitions |
|  |  |  |
| Additional Information: | | |

## Scenario Story #10

Realtor Compromise:

A local realtor’s database of clients and upcoming sales was compromised through a spear phishing attack. On the day of several closings, emails were sent to the realtors representing the buying parties that appeared to coming from the seller’s realtor. These emails stated that the seller would prefer all the proceeds be wired to a specific account instead of using a cashier’s check. On several occasions, realtors wired the proceeds and lost several hundred thousand dollars.

|  |  |  |
| --- | --- | --- |
| Use Case #10 | | |
| Title | Victim involved in Cyber Crime | |
| Category | Victim Notification | |
| Domain | * Cybersecurity * Law Enforcement | |
| Security Fabric  (e.g., U, LES, S, TS) | U, LES, S | |
| Scenario Description | Victim is directly involved in a cyber-enabled crime. This use case describes the situation where the victim is an entity or an organization where a specific criminal activity has been committed leading to emotional, physical or financial damage. | |
| COIs | * Federal↔State * Federal↔Citizen * Private↔Citizen * State↔Citizen * Citizen↔Citizen | |
| Key Stakeholders | | |
| Partners | SLTT Fusion Centers, SLTT Law Enforcement, FBI, CIKR/Private Sector | |
| Producers | SLTT Fusion Centers, SLTT Law Enforcement, FBI, CIKR/Private Sector | |
| Consumers | SLTT Fusion Centers, SLTT Law Enforcement, FBI, CIKR/Private Sector | |
| Scenario Details | | |
| Assumptions | Use of NIEM, use of STIX | |
| Exchange Scenario | * ABC bank reported an intrusion of their IT infrastructure where $X were directly stolen from specific bank accounts and transferred into a numbered account. * These funds were further redirected to other off-shore accounts, and cannot be traced anymore. * This is an example where a Victim is directly involved in a crime, and needs to be notified | |
| Business Rules | TBD by stakeholders | |
| Mapping to ESSA’s Enduring Functional Exchanges (EFE) | (1) Configuration/Anomaly Reporting; (2) Knowledge of Threat Actors; (3) Incident Awareness; (4) Indicators and Warnings; (5) Vulnerability Knowledge; (6) Mitigation Strategies; (7) Mitigation Actions & Responses. | |
| Data Elements | | |
| Action | Data Elements | Definitions |
|  |  |  |
| Additional Information: | | |

## Scenario Story #11

Narrative

|  |  |  |
| --- | --- | --- |
| Use Case #11 | | |
| Title | Victim Information Compromised | |
| Category | Victim Notification | |
| Domain | * Cybersecurity * Law Enforcement | |
| Security Fabric | U, LES, S | |
| Scenario Description | Victim information compromised as part of a cyber-intrusion. This use case describes the situation where the victim is one of a number of victims where their personal information has been compromised but no tangible damage has been inflicted (yet). | |
| COIs | * Fedederal↔State * Federal↔Citizen * Private Sector↔Citizen * State↔Citizen * Citizen↔Citizen | |
| Key Stakeholders | | |
| Partners | * SLTT Fusion Centers * SLTT Law Enforcement * FBI * CIKR/Private Sector | |
| Producers |  | |
| Consumers |  | |
| Scenario Details | | |
| Assumptions |  | |
| Exchange Scenario | * ABC bank also reported an intrusion of their IT infrastructure where SSNs, bank accounts, credit card numbers, and pins were stolen for 2 million users. * This is an example where private information of victims has been compromised, but no specific financial crime has been committed yet. * The victims still need to be notified and helped in a timely fashion the mitigate potential financial impact | |
| Business Rules |  | |
| Mapping to ESSA’s Enduring Functional Exchanges (EFE) | Refer to the ESSA identified Enduring Functional Exchanges [(1) Configuration/Anomaly Reporting; (2) Knowledge of Threat Actors; (3) Incident Awareness; (4) Indicators and Warnings; (5) Vulnerability Knowledge; (6) Mitigation Strategies; (7) Mitigation Actions & Responses]. Determine which EFE’s (1 thru 7) might be used during the scenario based upon the scenario’s participants. Each participant’s mission-specific operations will guide how many, and how much of each functions they are able to perform. | |
| Data Elements | | |
| Action | Data Elements | Definitions |
|  |  |  |
| Additional Information: | | |

## Scenario Story #12

A number of small businesses in X town, NY experienced cyber intrusion where music and software were purchased using stolen credit cards. The purchase amount for each one of these transaction were limited to $250. On further investigation it was determined that the music industry in general does not prosecute theft of music up to $275 per transaction (too expensive to prosecute, so they write-off the theft. Seems to be an insider who is aware of this practice and exploited to achieve their nefarious results.

|  |  |  |
| --- | --- | --- |
| Use Case #12 | | |
| Title | NCIJFT Cybercrime Investigation | |
| Category | Investigatory Referrals | |
| Domain | * Cybersecurity * Law Enforcement | |
| Security Fabric  (e.g., U, LES, S, TS) | U, LES, S | |
| Scenario Description | NCIJTF passes on an investigation of possible cybercrime with a nexus to an individual, organization, or critical infrastructure located within a State, to the State FC, as the thresholds for successful prosecution are not met at the federal level | |
| COIs | * Federal↔Fed * Federal↔State * State↔State | |
| Key Stakeholders | | |
| Partners | SLTT Law Enforcement, SLTT fusion centers, FBI , CIKR/Private Sector | |
| Producers | SLTT Law Enforcement, SLTT fusion centers, FBI , CIKR/Private Sector | |
| Consumers | SLTT Law Enforcement, SLTT fusion centers, FBI , CIKR/Private Sector | |
| Scenario Details | | |
| Assumptions | Use of NIEM | |
| Exchange Scenario | Scenario 2   * Local music companies collaborate to aggregate these thefts and develop a linkage pattern that links multiple transactions to the same IP address. * This helps them to now aggregate these transactions leading to higher transaction amounts and increased interest in reporting and prosecution   Scenario 3   * Local law enforcement is better able to serve their customers (local businesses) with these increased thresholds * They are able to escalate collections of cases to the State and Federal levels * FBI identifies that the same IP address committed similar crimes in multiple states and are not able to develop a campaign based on these referrals. | |
| Business Rules | TBD by stakeholders | |
| Mapping to ESSA’s Enduring Functional Exchanges (EFE) | (1) Configuration/Anomaly Reporting; (2) Knowledge of Threat Actors; (3) Incident Awareness; (4) Indicators and Warnings; (5) Vulnerability Knowledge; (6) Mitigation Strategies; (7) Mitigation Actions & Responses | |
| Data Elements | | |
| Action | Data Elements | Definitions |
|  |  |  |
| Additional Information: | | |

## Scenario Story #13

Researchers say they have discovered significant holes in the three key technologies sailors use to navigate: GPS, marine Automatic Identification System (AIS), and a system for viewing digital nautical charts called Electronic Chart Display and Information System (ECDIS). "Increasingly, the maritime domain and energy sector has turned to technology to improve production, cost and reduce delivery schedules," a NATO-accredited think-tank wrote in a recent report. "These technological changes have opened the door to emerging threats and vulnerabilities as equipment has become accessible to outside entities." Many cyber attacks have been carried out earlier on commercial ships, in one such incident a commercial ship on contract to the US military was the target of an intrusion by suspected Chinese military hackers. Another incident saw a major fuel supplier fall victim to an $18m scam as the bunkers sector faces growing cybercrime threats. In 2012, the Chinese military compromised “multiple systems” on a commercial ship on contract to Transcom. Marine shipping providers were also the target of so-called spear-phishing campaigns. These attacks use spoofed e-mails targeting a single company to gain secure access to confidential data. Similarly, KPMG has worked with one major shipping company that has been a victim of a deliberate hacking attack, possibly by a rival. Hackers recently shut down a floating oil rig by tilting it, while another rig was so riddled with computer malware that it took 19 days to make it seaworthy again; Somali pirates help choose their targets by viewing navigational data online, prompting ships to either turn off their navigational devices, or fake the data so it looks like they’re somewhere else; and hackers infiltrated computers connected to the Belgian port of Antwerp, located specific containers, made off with their smuggled drugs and deleted the records. For example on a Friday afternoon, freight needs to move, fast. A shipper, frantic to find a transporter, hooks up with a carrier on a load board. They agree to terms, and a ship is dispatched to pick up the load. The only problem is that ship isn’t from the party that accepted the load. That “company” double-brokered the shipment to a legitimate shipper. The load goes one way, the money goes another, and the vessel that delivers the freight winds up with nothing.

|  |  |  |
| --- | --- | --- |
| **Use Case #13** | | |
| **Title** | **Maritime Containerized Cargo Operations** | |
| **Category** | Integrated Threat Assessment for Critical Infrastructure | |
| **Domain** | * Cybersecurity * Physical Infrastructure Protection * Law Enforcement * Intelligence Community | |
| **Security Fabric**  **(e.g., U, LES, S, TS)** | SBU | |
| **Scenario Description** | Cargo operations at U.S. ports of entry are critical to our overall national security and a component of the DHS strategic priority to “minimize the disruption to and facilitate the safe and secure inbound and outbound legal flows of people and goods.”  A 2013 economic impact assessment of U.S. west coast ports found that ILWU terminals support 9.2 million workers who received $383.1 billion in wages and salaries. The cargo transiting the west coast  ILWU terminals generated $2.1 trillion, which represents 12.5% of the U.S. GDP (2014). The valuable role that seaports play in our economy makes them a target.  A successful nuclear terrorist attack on a U.S. seaport has been estimated to result in “disruption of U.S. trade valued at $100-200 billion, property damage of $50-500 billion, and 50,000-1,000,000 lives.” | |
| **COIs** | FSLTIPP stakeholders in the port system, including but not limited to:   * Federal agencies, e.g., CBP, USCG; * State and local authorities, e.g., fire, police; * Port authorities, e.g., Port of Seattle; * Labor unions, e.g., ILWU; * Non-governmental organizations, e.g., pilots associations, towage; * Customers, e.g., importers; and industrial partners. | |
| **Key Stakeholders** | | |
| **Partners** | CPB, USCG, NIMO, | |
| **Producers** | Port authorities, and Maritime | |
| **Consumers** | State and local authorities, fire and police | |
| **Scenario Details** | | |
| **Assumptions** | Given the scenario description, a successful nuclear terrorist attack on a U.S. seaport has been estimated to result in “disruption of U.S. trade valued at $100-200 billion, property damage of $50-500 billion, and 50,000-1,000,000 lives.” Use of NIEM, use of STIX | |
| **Exchange Scenario** | XXXXXXXXXXXXXXX – Need specific information exchanges  Through a critical review of the as-is model of information flow that enables the cargo movement workflow, we uncovered information dependencies among different operational divisions at the terminal (e.g., security and operations) as well as between the terminal and outside agencies. | |
| **Business Rules** | TBD by stakeholders | |
| **Mapping to ESSA’s Enduring Functional Exchanges (EFE)** | Refer to the ESSA identified Enduring Functional Exchanges [(1) Configuration/Anomaly Reporting; (2) Knowledge of Threat Actors; (3) Incident Awareness; (4) Indicators and Warnings; (5) Vulnerability Knowledge; (6) Mitigation Strategies; (7) Mitigation Actions & Responses]. Determine which EFE’s (1 thru 7) might be used during the scenario based upon the scenario’s participants.  Each participant’s mission-specific operations will guide how many, and how much of each functions they are able to perform. | |
| Data Elements | | |
| Action | Data Elements | Definitions |
|  |  |  |
| Additional Information: | | |

Narrative

|  |  |  |
| --- | --- | --- |
| Use Case #14 | | |
| Title | State Cybercrime Investigation | |
| Category | Deconfliction of (cybersecurity threat) indicators | |
| Domain | * Cybersecurity * Law Enforcement * Critical Infrastructure | |
| Security Fabric  (e.g., U, LES, S, TS) | U, LES, S | |
| Scenario Description | Cybercrime investigation at the state level develops law enforcement sensitive information around specific cybersecurity indicators. Current professional best practice is to deconflict both operational activity (location/event) as well as case entity. This is well developed around people and person centric indicators. As these indicators existing in cyberspace, there is a pressing need to interoperate. | |
| COIs | * Fed↔Fed * Fed↔State * Fed↔International * State↔State | |
| Key Stakeholders | | |
| Partners | * SLTT Law Enforcement, * SLTT emergency management * SLTT fusion centers * FBI * CIKR/Private Sector | |
| Producers |  | |
| Consumers |  | |
| Scenario Details | | |
| Assumptions |  | |
| Exchange Scenario | * Local music/software companies report unauthorized downloads of music/software from a specific collection of IP addresses * State Police and FBI review these IP addresses and identify similar IP addresses used in other states also * The National Cyber centers report same IP addresses also logged attempting to infilterate a large defense contractor looking for designs for the latest F35 fighter jet * Infraguard reports the IP address popping up in a number of chat rooms with malicious propaganda * DHS S&T reports a number of new RFIs initiated about these same IP addresses * All these incidents have to be deconfliced, and all responses coordinated to reduce overlap, confusion, and other covert operations. | |
| Business Rules |  | |
| Mapping to ESSA’s Enduring Functional Exchanges (EFE) | Refer to the ESSA identified Enduring Functional Exchanges [(1) Configuration/Anomaly Reporting; (2) Knowledge of Threat Actors; (3) Incident Awareness; (4) Indicators and Warnings; (5) Vulnerability Knowledge; (6) Mitigation Strategies; (7) Mitigation Actions & Responses]. Determine which EFE’s (1 thru 7) might be used during the scenario based upon the scenario’s participants. Each participant’s mission-specific operations will guide how many, and how much of each functions they are able to perform. | |
| Data Elements | | |
| Action | Data Elements | Definitions |
|  |  |  |
| Additional Information:  Specific data elements are not available, but here are the ‘types’ of information that may be exchanged to meet the requirements for this use case (depending on the level of detail available at the time of publication of the intelligence product): (1) Details about the event including where and when observed, behavior indicators, etc.; (2)  Specific details about the malware, behavior if available; (3) Mitigation strategy; (4) Mitigation steps; and (5) Acknowledgement of receipt and confirmation of execution of steps | | |

Appendix A— Enhanced Shared Situational Awareness (ESSA) Information Exchanges

ESSA attempted to capture and categorize all major activities that are associated with cybersecurity information sharing at the Federal Government level, realizing that those involved in the cybersecurity mission space could benefit from each other’s shared experiences - and should do so. EFEs are categories of information that are exchanged on an ongoing basis to promote and enhance cybersecurity information sharing and shared situational awareness. Within each EFE, there are a series of subcomponents that represent various data types. In short, the following EFEs are a series of information exchanges to collectively describe the information needed to support a cybersecurity information sharing model.

|  |  |  |  |
| --- | --- | --- | --- |
| **EFE #** | **EFE Name** | **Subcomponent ID** | **Subcomponent Name** |
| **1** | Configuration / Anomaly Reporting | 1a | Risk Posture |
| 1b | Anomalies |
| 1c | Infrastructures |
| **2** | Knowledge of Threat Actors | 2a | Threat Actor Infrastructure |
| 2b | Threat Actor Personas |
| 2c | Threat Actor Attribution |
| 2d | Trend Analysis |
| 2e | Victim Information |
| 2f | Threat Actor Indicators |
| **3** | Incident Awareness | 3a | Incident Information |
| 3b | Computer Network Operations (CNO) Awareness |
| 3c | Incident Data |
| 3d | Infrastructure Impact/Effects |
| 3e | Victim Information |
| 3f | Alerting Indicators |
| **4** | Indications and Warnings | 4a | Events and Alerts |
| 4b | Warnings |
| 4c | Impact Assessments |
| 4d | Potential Indicators |
| **5** | Vulnerability Knowledge | 5a | Vulnerabilities |
| 5b | Exploits |
| 5c | Potential Victim Information |
| **6** | Mitigation Strategies | 6a | Coordinated Action Plans |
| 6b | Courses of Action |
| 6c | Understanding of Achievable Mitigation Effects |
| **7** | Mitigation Actions and Responses | 7a | Tasking and Status |
| 7b | CNO Capability Awareness |
| 7c | Effectiveness Reporting |
| 7d | After-Action / Lessons Learned Information |

Appendix B— Document History

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Editor** | **Change** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Appendix C—Fusion Center Cyber Information Sharing

#### Fusion Center Cross-Domain Sharing

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Use Case Description | | | | | | | | | | |
| Title | | Fusion Center Cross-Domain Sharing | | | | | | | | |
| Organization | | Fusion Center | | | | | | | | |
| Security Classification | | Law Enforcement Sensitive | | | | | | | | |
| Use Case Description | | This use case describes scenarios where a fusion center supports multiple communities by bridging gaps in structure, format, protocol, and vocabularies to communicate intelligence products that may alert the community to a cross-domain incident while it is happening, or provide a more detailed product that advises the community about the issues, provides indicators that the community of practitioners may leverage to track the anomaly, or provide more detailed recommendations on mitigation strategies, or actions that the community could take to help address the issue | | | | | | | | |
| COIs | | | | | | | | | |
| P<>F | P<>S | | | P<>I | F<>S | | F<>I | S<>I | P<>P |
| F<>F | S<>S | | | I<>I | F<>C | | P<>C | S<>C | C<>C |
| Key Stakeholders | | | | | | | | | | |
| Producers | |  | | | | | | | | |
| Consumers | |  | | | | | | | | |
| Use Case Details | | | | | | | | | |
| Assumptions | | |  | | | | | | |
| Exchange Scenario | | | PROBLEM/INCIDENT  Wayland PD: Computer Crime Targeting Municipalities - Forward to IT Units  Recently, the Town of Wayland, MA became a victim of a computer crime, in which, suspect(s) were able to access one of the Town of Wayland's bank accounts and attempted to wire $4,365,365.94 in three wires to China and Mongolia.  Thankfully, the wires were not completed.  During the initial investigation, the IT department had located an email that contained 2 viruses sent from an outside Auditor to employees of the town.  At least one town employee opened the email and subsequently, malware was detected on the Towns server.  The two malware files that you/your towns/cities should be aware of are:  Trojan.Email.FakeDoc and Spyware.Dyre  It is believed that what appears to be a bank website is a copy of one and once you input your login and password it is captured.  The Wayland Police Department is working with the FBI Boston Division on this investigation.  The FBI reports that this complex criminal activity has not been seen in the Boston area before.  I am trying to get the word out so that other towns/cities do not fall victim.   ASCIA FOLLOW UP QUESTIONS                  •       How was the malware detected on the server? •       Was the email account that received the malicious email web based or client based? •       Did the computer network have software / filters to identify suspect email attachments? •       Where does the fake bank website resolve to / was a domain search done? If so, can we trace it to a server or payment source? Keep in mind that although the investigation may resolve out of county, the server may be located somewhere in the US and someone is paying for that service. •       What did the advanced email headers of the email reveal?Where did it come from (IP)? •       Does the town have a policy that addresses opening email from an unknown source?  RESULTS FROM FOLLOW UP •       A user on the network reportedly opened an email that was from an outside contractor/auditor and did not open the attachment. •       The town treasurer reportedly then received an email (from the user who deleted the email and was an employee) that was not opened and deleted it without opening the attachment. •       The town treasurer then visited what he thought was the bank website which he tried to login.  The website said there were issues try back later. •       The town treasurer then received a call from what he thought was the bank verifying information for wire transfers, which he provided. •       A short time later the treasure then received an actual fraud call from the bank whereby he was asked why he was transferring money to China. •       At this point, the breach was determined. •       The FBI was involved in the breach and now stands at a lower priority since the funds were not lost. •       All machines were scanned and the malware was found.  The FBI was determining more information on ip addresses and destinations. •       Now, pro-actively all machines are scanned daily for anti-virus and malware. | | | | | | |
| Business Rules | | |  | | | | | | |
| Data Elements | | | | | | | | | | |
| Action | | Data Elements | | | | Definitions | | | | |
|  | |  | | | |  | | | | |
| Specific data elements are not available, but here are the ‘types’ of information that may be exchanged to meet the requirements for this use case (depending on the level of detail available at the time of publication of the intelligence product)   * Details about the event including where and when observed, behavior indicators, etc. * Specific details about the malware, behavior if available * Mitigation strategy * Mitigation steps * Acknowledgement of receipt and confirmation of execution of steps | | | | | | | | | | |

1. It is important to note the cross domain use cases described in this document seek to align with the on-going efforts of the Federal Government’s The Enhanced Shared Situational Awareness (ESSA) activity that was initiated in 2010 to support planning, development, and implementation of a cybersecurity information sharing architecture that defines the functions, activities, and information exchanges within and among the Federal Government’s Cybersecurity Centers. The information exchanges identified through the ESSA effort are defined in terms of “enduring functional exchanges (EFE). Within each EFE, there are a series of subcomponents that represent various data types. EFEs are categories of information that are exchanged on an ongoing basis to promote and enhance IOA, planning, and multiple levels of SSA. These categories contain a number of more specific information flows that would feed or be produced by center processes. The seven EFEs are as follows and are further defined in Appendix A. [↑](#footnote-ref-1)