Task Force on Optimal PSAP Architecture

An FCC Federal Advisory Committee

December 2, 2016

WORKING GROUP 1

Optimal Cybersecurity Approach for PSAPs

Supplemental Report

Table of Contents

1 Introduction

On October 26, 2016, multiple Public Safety Answering Points (PSAPs) in twelve States experienced sporadic, but targeted, Telephone Denial of Service (TDoS) attacks. These attacks were the first ever to directly target "9-1-1" instead of administrative lines supporting the PSAPs. Fortunately, these attacks did not disable any PSAPs, but they did impact operations and delay calls, and likely responses, as a result. This most basic of attacks was levied not against Next Generation 9-1-1 systems, and not even against legacy systems in the transitional phase, but instead the attack impacted every type of PSAP regardless of technological makeup. It did so by using wireless phones to do exactly what it was designed to do, dial "9-1-1". Without going into great detail, the particular vector of this attack used a well known social media site to send a hyperlink to an Internet site, and upon clicking on the link, the users wireless phone was, unbeknownst to the user, infected with malware that instructed the phone to auto-dial 9-1-1 repeatedly. This occurred in the background with no obvious visible evidence to the user. Most users only found out when the PSAP they had dialed, and were still dialing, was able to call them back and ask if they had an emergency.

The demonstrated ability of an individual, or small group, to impact our Nation's 9-1-1 networks, systems and facilities, even in their current legacy state, reinforces the fact that we can no longer take Cybersecurity for granted. We can not afford to ignore the fact that cyber attack against our 9-1-1 system is a very real risk. Not only is it a risk, it is here and it is already happening. In our quest to ensure that future networks are defended we must also remember to protect the entire network, as an enterprise, or be prepared to deal with an infiltration of the weakest link.

This report is the second, and final, report of TFOPAs Working Group 1. As with the original report, many of the themes underlying these discussions, and this report, are drawn from work completed or underway by National Institute of Standards and Technology (NIST), Department of Homeland Security (DHS), Association of Public-Safety Communications Officials (APCO), National Emergency Number Association (NENA), and other relevant authorities.

In its first report[1], WG1 proposed a cooperative and synergistic approach to cybersecurity for public safety communications, including core cybersecurity services; interconnected monitoring and mitigation; and near real-time information sharing amongst multiple levels of public safety agencies and entities. WG1 also included examples of alternative models, and partnerships to be considered, along with high-level pricing estimates. The intent of this supplemental report is to expand upon specific areas of the initial report focusing on the Emergency Communications Cybersecurity Center or EC3.

In this supplementary report, WG1 has provided expanded cost estimates to include implementation of proposed cybersecurity options at the local, State and Regional levels and operational costs based on graded levels of service and traffic. The WG also expands on the previous recommendations of incorporating various types of sensors and monitoring into the overall approach for cyber defense. In addition, and critical to the success of any cybersecurity effort, the WG provides examples of, and links to, specific information sharing environments (ISEs) that currently exist which can be utilized to the benefit of public safety communications at little or no cost. The WG also extends the discussion to include information sharing options

[1] FCC, Task Force on Optimal PSAP Architecture, https://transition.fcc.gov/pshs/911/TFOPA/TFOPA_FINALReport_012916.pdf.

and recommendations to include partnerships between Federal and State, Local, Tribal and Territorial (SLTT) agencies and entities.

The WG then provides recommendations for near, mid, and long term considerations and actions believed important to PSAPs and public safety in general. The recommendations are intended to be advisory in nature, and are complementary to the planning, deployment, and operation of EC3s.

Finally, in anticipation of potential future work, the WG provides a list of suggested follow on topics and recommendations for additional research and reporting. This list is provided for many areas that WG1 simply did not have the time, or resources, to address during the initial charter of TFOPA.

1.1 Working Group 1 Team Members

Name	Organization/Company
Tim May (Designated Federal Officer)	Federal Communications Commission
Dana Zelman (FCC Liaison)	Federal Communications Commission
Steve Souder (TFOPA Committee Chair)	Fairfax County, VA
Dana Wahlberg (TFOPA Committee Vice- Chair)	Minnesota Department of Public Safety
Jay English (WG 1 Chair)	Association of Public Safety Communications Officials
David Holl (WG 2 Chair)	PA Emergency Management Agency
Jim Goerke (WG3 Chair)	Texas 9-1-1 Alliance
Mary Boyd	Intrado
Drew Morin	T-Mobile
April Heinze	Indigital
Robert Brown	National Public Safety Telecommunications Council
Anthony Montani	Verizon
Dusty Rhoads	Department of Homeland Security
Susan Nelson	Public Service Commission, District of Columbia
Michael Kennedy	Office of Director of National Intelligence
Tim Lorello	SecuLore
Jeanna Green	Sprint

Table **1** - List of Working Group Members

2 Objectives as assigned for second report

2.1 Objective

Upon completion of the initial reports, the three Working Groups (WGs) of the Task Force on Optimal PSAP Architecture (TFOPA) were tasked with follow on work. The specific tasking to WG1 was as follows:

In-Depth Review of Emergency Communications Cybersecurity Center (EC^3) Concept

> The Task Force adopted WG1's recommendation calling for creation of an additional PSAP security layer known as the Emergency Communications Cybersecurity Center (EC^3). The Task Force will conduct in-depth study of this model, including what operations and costs might look like if established on local, state or regional level; alternative solutions that achieve the same end goal and their associated costs; and specific opportunities for the EC^3 to integrate efficiently with the DHS National Cybersecurity & Communications Integration Center (NCCIC) and Multi-State Information Sharing & Analysis Center (MSISAC) models. The Task Force would also make specific recommendations with respect to how identity, credentialing and access management (ICAM) would be addressed in the EC3 environment.

2.2 Scope

The scope of this work is limited to expanding on the proposed EC3 model and specifics as to what options might be available to the public safety and 9-1-1 community for implementation of that model. However, in researching current areas for improvement with regard to public safety communications cybersecurity, the WG also determined that incorporation of existing Information Sharing Environments (ISEs), and the exploration of various existing options, would be inline with tasking. As a result, both are examined in this report.

2.3 Methodology

The WG determined that presentations from various potential providers of like services would be of value. As a result, invitations were issued to a number of potential industry partners. Only two (2) companies accepted the invitation to present. However, both of these organizations were key partners in the initial proposed architecture and both provided additional details and implementation specifics. These two companies, Critical Informatics who provides the ECATS system mentioned in the original report, and CIS, the provider of MS-ISAC services, were helpful in exploring the EC3 concept at a deeper level.

Once the WG had received presentations from these two organizations there were additional presentations from the DHS Office of Emergency Communications (OEC) on the updated to the NIST Cybersecurity Framework, and from the Office of the Director of National Intelligence (ODNI) on existing information sharing opportunities. All of the information gleaned from these presentations is included in some form in this supplemental report.

3 The EC3 Concept

The Emergency Communications Cybersecurity Center (EC3)

As part of the initial, approved, report submitted to the Commission, WG1 determined that an additional element should be introduced into the recommended future architecture. As a result, a logical architecture was developed to illustrate the potential functions and capabilities of this new element. The group agreed to naming this element the Emergency Communications Cybersecurity Center, or EC3. The intent of the logical architecture recommendation is to create a centralized function, and location, for securing Next Generation (NG) networks and systems. By centralizing certain features, including cybersecurity in general, and intrusion detection and prevention services (IDPS) specifically, public safety can take advantage of economies of scale, multiple resources, and systems and best practices which may already be in place or at a minimum readily available for deployment and use.

This concept is intended to empower Federal, State, local, tribal and territorial (FSLTT) PSAPs and 9-1-1 authorities, by providing cooperative options to defend both common areas of interest and individual networks and systems. Through the establishment of certain shared core services like cybersecurity, which can be utilized by multiple participating agencies, agencies can realize substantial cost savings and could also decrease the time needed to implement a comprehensive cybersecurity system.

The information collected by the EC3s that relates to the PSAPs will be the result of the monitoring that the center will conduct. As a result, it will be necessary to deploy some type of sensors at all PSAP locations. As part of the design, and implementation consideration, a way will need to be devised to get traffic to funnel through a centralized "cyber core" function. In our proposed model, the EC3 can serve this function for multiple PSAPs and provide monitoring at a regional or State level. Similar in concept to the DHS Einstein program, the EC3 would be specific to public safety communications, performing many of the same functions as Einstein. It might also be useful to consider the Einstein model for design, and perhaps even pricing, considerations. More information on Einstein can be found at: https://www.dhs.gov/einstein.

In the WG1 proposed model, as various PSAPs subscribe to an EC3, the information and intelligence gleaned from this monitoring becomes shared, and mutually protected. Multiple EC3s could then be linked together, and used to aggregate the traffic. At this point, shared intelligence would be possible between EC3s (and the agencies they serve) along with designated FSLTT partners. The proposed location of the EC3, within an NG9-1-1 system, seems to logically be best accomplished at the Emergency Services IP Network (ESInet) level. Since there are other NG9-1-1 Core services required, and they will also utilize the ESInet for transport, and since the ESInet provides the needed connectivity to, and between, multiple PSAPs and the core NG9-1-1 services, placement of the IDPS services, in the form of the EC3, at the ESInet layer would provide the most visibility to critical traffic and afford the broadest protection to all partners.

Proposed Approach for Intrusion Detection and Preventions System (IDPS) in the NG9-1-1 Environment

In the proposed NG9-1-1 architecture, the EC3 will take on the role of providing IDPS services to PSAPs and any other public safety communications centers (PSCC), services, or systems that would consider utilizing the centralized, core services architecture proposed. For example, not only PSAPs but Emergency Operations Centers (EOCs), Fusion centers, and potentially the Nationwide Public Safety Broadband Network operated and maintained by

FirstNet, could also interconnect to the EC3 service. This approach would allow public safety to build one infrastructure and use it for many clients. This provides significant economies of scale, puts multiple FSLTT resources into the same protection scheme, and allows for sharing of data, mitigation strategies, and recovery efforts across enterprise.

The potential flow of this system would begin with the Originating Service Provider (OSP) and NG9-1-1 Core Services elements, would encompass the ESInet transport network within and between disparate PSAPs and would provide for monitoring of call statistics, system health, anomaly detection, data sharing, mitigation and recovery while still allowing local agencies to maintain local control of day to day operations within their specific PSAPs. Rather than requiring PSAPs to build and staff such facilities, the EC3 concept allows for PSAPs from within and across jurisdictions, to interconnect to the core cybersecurity system and benefit from its capabilities, whether federal, state, local, tribal or territorial. While not specified herein, the interconnect requirements would include cyber hygiene due diligence elements at the PSAP, single user sign on and multi-factor authentication at the local levels and some form of agreed upon, trusted connection (and relationship) from the local levels to the State or Regional level EC3. This architecture is also intended to represent a scalable, and customizable, approach. This means for localities with larger than average emergency communications systems (major metropolitan areas such as New York, Los Angeles, *etc*.) there is ample opportunity to construct a single EC3 to serve this individual customer. However, any EC3 should be designed and constructed in such a way that it will interconnect with other EC3's throughout the United States with the same functions, requirements and failover capacity as addressed in more detail in the first TFOPA report. From the regional or State level, the information should flow to a centralized repository with adequate service capabilities to support multiple clients, and incidents, in real time.

In the WG1 proposed model, as various PSAPs subscribe to an EC3, the information and intelligence gleaned from this monitoring becomes shared, and mutually protected. Multiple EC3s could then be linked together, and used to aggregate the traffic. At this point, shared intelligence would be possible between EC3s (and the agencies they serve) along with designated FSLTT partners. The proposed location of the EC3, within an NG9-1-1 system, seems to logically be best accomplished at the Emergency Services IP Network (ESInet) level. Since there are other NG9-1-1 Core services required, and they will also utilize the ESInet for transport, and since the ESInet provides the needed connectivity to, and between, multiple PSAPs and the core NG9-1-1 services, placement of the IDPS services, in the form of the EC3, at the ESInet layer would provide the most visibility to critical traffic and afford the broadest protection to all partners. Some examples of how this data flow, and cooperative approach, might present are included in Figures 1 and 2 on the following pages.

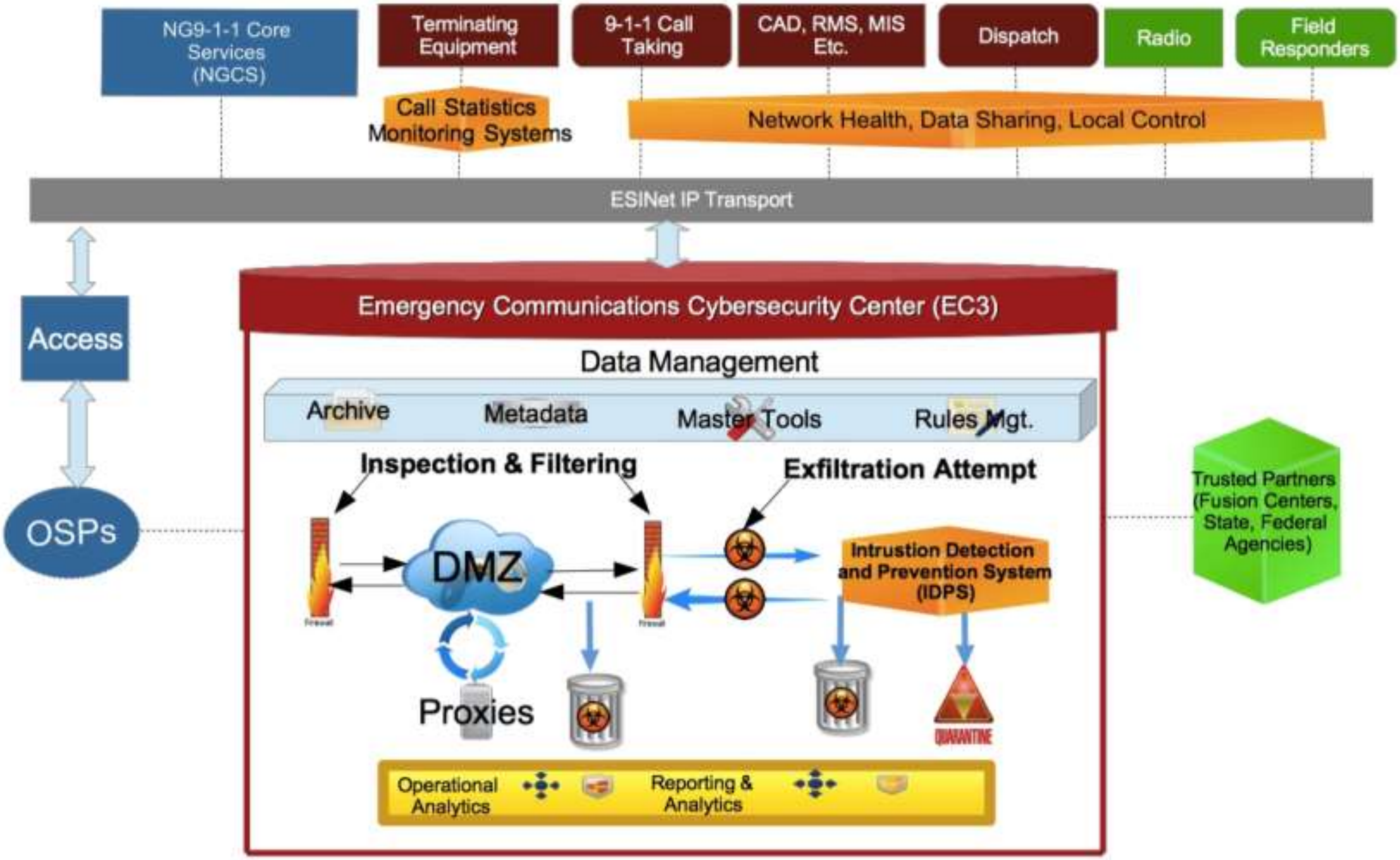


Figure 1 - The Emergency Communications Cybersecurity Center (EC3)

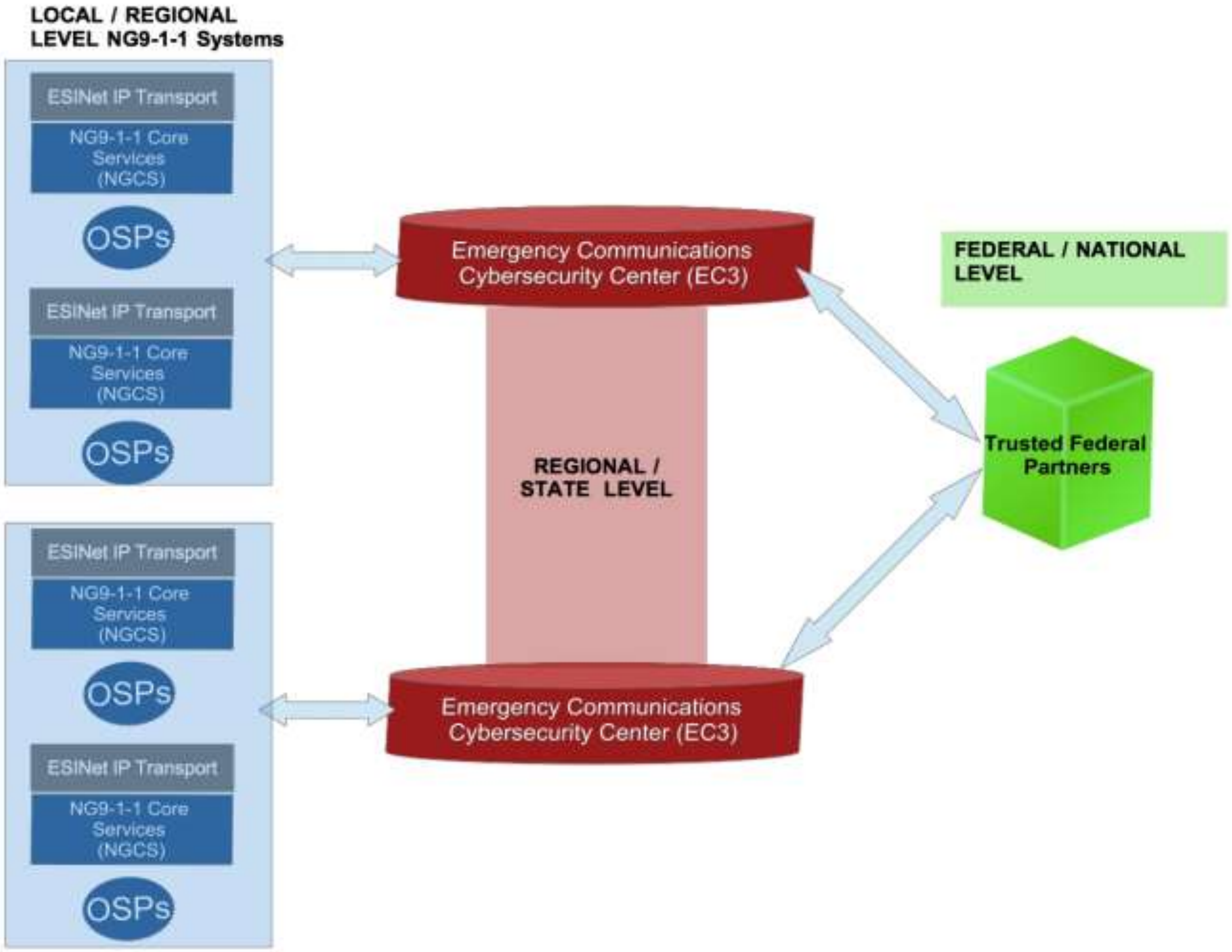

LOCAL / REGIONAL LEVEL NG9-1-1 Systems
ESINet IP Transport
NG9-1-1 Core Services (NGCS)
OSPs
ESINet IP Transport
NG9-1-1 Core Services (NGCS)
OSPs
ESINet IP Transport
NG9-1-1 Core Services (NGCS)
OSPs
ESINet IP Transport
NG9-1-1 Core Services (NGCS)
OSPs
Emergency Communications Cybersecurity Center (EC3)
REGIONAL / STATE LEVEL
Emergency Communications Cybersecurity Center (EC3)
FEDERAL / NATIONAL LEVEL
Trusted Federal Partners

Figure 2 – EC3 shared data flow example

4 Operationalizing the EC3 – Options and Opportunities

4.1 Implementation Considerations

As previously noted, WG1 will not delve into specific architecture discussions. However, in considering deployment options, it is important to note that there must be commonality of certain network elements, cybersecurity functions, and core NG9-1-1 systems. While the WG is not proposing a federalized model, is it important to consider the need to share certain core systems, functions, and data and a much larger level than current operations allow. To this end, the creation of a single EC3 to serve multiple PSAPs, and the need to interconnect all EC3's in order to share information in real time is critical to success. To this end, the creation of EC3's to serve multiple PSAPs, and the need to interconnect all EC3's in order to share information in real time is critical to success.

As cybersecurity risks and capabilities evolve, it will become even more critical to employ a system that will learn the spatiotemporal patterns of data, communications, and application usage in given roles and scenarios and then identify anomalous behaviors that may be indicative of a threat to network security.

4.1.1 Deployment of network sensors

As detailed in the original WG1 report, one current model upon which to base future design and implementation considersions utilizes the deployment of network sensors. This automated process of collecting, correlating, and analyzing computer network security information across State governments can be used as a model for the interconnection of EC3s to both each other, and to Federal partners such as DHS-NCCIC and the FCC. It should be reiterated that WG1 is not endorsing any specific vendor, product, or organization. The model provided is useful and an appropriate case study for future implementation considerations.

As currently deployed in one model, the sensors incorporate a netflow and Deep Packet Inspection (DPI) based monitoring solution. It has two main functionalities:

- Monitor the raw packet stream and converts it into a flow format for efficient storage and historical analysis
- Leverage high performance Intrusion Detection System (IDS) engine for accurate malicious event identification and reporting

The solution leverages four main signature sources which are:

- Professional services signature feed purchased through vendors
- Advanced Persistent Threats (APT) indicators
- Center for Internet Security Incident Response Indicators
- Intel and Security Researchers

In order to effectively monitor networks and notify users of potential anomalies or breaches, the solution needs to tap into the raw network traffic. This can be accomplished with a network tap or a span port on the core switch. A TAP (Test Access Point) is a passive mechanism installed between a "device of interest" and the network. TAPs transmit both the send a receive data streams simultaneously on separate dedicated channels. This insures that all of the data arrives at the monitoring device in real time. A SPAN is a Switch Port Analyzer port,also known as a mirror port. An analysis device can be attached to the SPAN port to access network traffic reducing cost and capturing intra-switch traffic. Both have pros and cons and both are viable options depending on network set up and monitoring and maintenance requirements.

In addition, and in order to facilitate monitoring, the solution needs two ports opened on the customer firewall.

IP Monitoring can be conducted on a variety of targets of interest to include:

- IPs connecting to malicious C&Cs
- Compromised IPs
- Indicators of compromise
- Notifications

In addition, the solution offers domain monitoring which includes notifications on compromised user credentials, open source and third party information and a vulnerability management Program.

The general idea behind the deployment of these types of sensors is that at some point, an infected system is going to have to reach out to a host on the Internet to receive additional commands, download additional software, or exfiltrate information. Monitoring an organization’s Internet connection is an effective way to get visibility into their network. The limitation here is that there may not be good visibility on internal to internal communication.

While this is typically not a concern as most of the attacks and compromises originate from, or beacon out to, the Internet at some point. Setting up the PSAPs so that an EC3 would essentially function as their ISP would be an effective way to have eyes on that type of traffic.

4.1.2 The CalOES approach – Wireless environment sensor deployment

In addition to the deployment of network sensors, consideration should be given to a model currently in use by the State of California’s Office of Emergency Services (CalOES). This system is comprised of a “phased array” approach with sensors deployed at each PSAP in the State that monitor traffic from both wireline and wireless communications sites. Specifically these sensors, which are currently deployed and actively monitored by both CalOES and the DHS NCCIC, provide a near real time picture of the health and status of every wireless site, and system, responsible for providing wireless connectivity to the public and wireless 9-1-1 traffic to the PSAPs.

The mission of the federal government’s emergency communications charter (to ensure that relevant federal, state, local, tribal and territorial officials can continue to communicate in the event of a catastrophic loss of communications) can be seen as largely dependent on the federal government’s ability to understand mission impacts on emergency communications. It is imperative that this is done in a timely manner so that coordinated response and recovery efforts get to those systems in time. Sensors and business processes, providing visibility into those systems, enabling rapid assimilation of critical emergency communications impacts to state, local and tribal governments by the federal government currently do not exist in an effective manner.

The California Governor's Office of Emergency Services (CalOES) proposed leveraging an existing sensor system deployed within PSAPs in California. This system can be used to support the mission of protecting the PSAPs against cyber-attacks and physical disaster response and was seen as an additiona method of ensuring continuity of emergency communications during major crisis or disaster.

The sensor system network enables real-time visualization of call data, without any Personally Identifiable Information (PII), which can alert a monitoring center to a disruption to 9-1-1 services by the Local Exchange Carrier, or named wireless service providers, as observed in Virginia during the Derecho, or after an Earthquake. CalOES, in an unprecedented effort to share real-time data with the federal government for disaster management purposes, has developed a demonstration concept with the National Coordination Center for Communications (NCC), which could provide the basis for defending the enterprise of PSAPs against emerging cyber threats, or attempts by terrorists to disrupt public safety communications during a coordinated domestic attack against the homeland, or simply improve response coordination for disaster communications restoration after a natural disaster.

The NCCIC, in partnership with CalOES is capable of providing constant and continual monitoring of the ECATS dashboard, deployed by CalOES across the entire State of California. In this capacity the NCC and NCCIC can coordinate with CalOES, Federal Bureau of Investigation (FBI), and other government agencies and telecommunications service providers in the event of an anomaly across one or many PSAPs. Additionally, use of this Local-State-Federal partnership model enables a coordinated, and unified, restoration effort in the event of loss of connectivity. This model also provides monthly reports of incidents, and outcomes, along with investigative assistance and coordination of lessons learned via after action reports involving all stakeholders.

4.1.3 Voice and Data Monitoring – Both are critical

The monitoring of both voice and data networks that feed the 9-1-1 system, and of the data systems within and between PSAPs is of great importance and can be accomplished via a combination of mechanisms. In addition to monitoring, mitigation is a key element in the overall function, and goal, of the EC3 concept. The EC3 will likely be tasked with identifying threats, explaining why they are of concern, and making recommendations to the affected PSAPs for steps to mitigate the threat.

Most of what is seen in current Security Operations Centers is tied back to malware infections that can either be cleaned or the systems re-imaged entirely. It will also become important to track any incidents that are escalated to the PSAPs in some form of ticketing system for tracking and reporting services. In addition, it would be most effective if there was a method to correlate all the alerts generated by deployed sensors across all EC3s in order to identify any trending related to the top threats facing the PSAPs.

Depending on the specific needs of the PSAPs, not every EC3 may need to have every service available to it. As an example, computer forensics services may not be a requirement at each EC3. Perhaps only the larger EC3s in the large urban areas throughout the country may have forensics capabilities and the EC3s could coordinate to send forensic images for analysis along to those designated EC3s. Likewise, certain reporting capabilities and aggregate products could be handled by either larger, regional EC3's or even by trusted Federal partners or both.

Potentially, all of the data from the sensors would route back to the NCCIC, FCC Operations Center, or similar facilities, for analysis and escalation back out to the EC3s. As the system continued to build out monitoring infrastructure, it would become easier to correlate data across multiple partners and start to paint the picture of how new attacks and threats evolve as they begin to affect the various SLTT entities being monitored.

4.2 Estimating Costs – Capital and Operational

4.2.1.1 Capital Costs and Considerations

The building out of the EC3 should be a very similar per foot cost as compared to the building out of normal office space which typically includes cubicles and workstations for analysts. There may be some additional costs incurred for flat panel displays and a computer systems to drive them. As a result, while the working group cannot provide a definitive estimate for what an EC3 physical build out might cost, as these costs may vary widely, the group does believe that the guidelines provided should allow local, regional, tribal and State decision makers to have a starting point from which they can at least begin estimates based on local cost factors.

In addition to building, repurposing, or co-locating at existing data and/or security centers, a physical buildout, and capital expense, will be necessary for the deployment of sensors at the EC3s. At a high level, it would make the most sense to deploy an "Albert like" sensor at each EC3, as the EC3s (ideally) would be the aggregation point of all PSAP network traffic. These sensors are essentially commodity hardware and typically cost between $6,000 – $12,000 depending on the throughput of the network that is being monitored. For example, a $12,000 sensor would be more than capable of monitoring a 10GB network with an average utilization of 6-8GB. In addition, and as previously discussed, it would also be recommended that consideration be given to deployment of a sensor system similar to that in use by CalOES.

Based on input from a provider of equipment and services for the CalOES model, who is engaged in current cybersecurity operations, and a participant in the TFOPA WG1 presentations, Table 2 shows a high level estimates for deployment of such sensors can be included. This would be cost for a single EC3 serving multiple (2-20) PSAPs.

Table 2 – High Level Cost Estimate of Sensor Deployment

Sensor Related Cost Elements	Cost	Quantity	Total Estimate
License	$100,000.00	1	$100,000.00
Sensors	$5,000.00	40	$200,000.00
Sensor Maintenance	$1,000.00	40	$40,000.00
Data Center Servers - Hardware	$7,500.00	10	$75,000.00
Data Center Servers - Maintenance	$1,500.00	10	$15,000.00
SOC Analyst Training (2 People $200.00/Hr)	$400.00	240	$96,000.00
IT resource training (hours)	$200.00	80	$16,000.00
Estimated total			**$542,000.00**

As with any cost estimates, these will likely vary widely based on location, availability of existing data center resources, physical construction, and the decision as to what size and level of service an organization, or group or organizations, would ultimately pursue. It should be noted again that there is a tremendous opportunity to realize economies of scale by centralizing certain core functions, like cybersecurity, and sharing the EC3 resources amongst multiple partner agencies and organizations. This will realize individual savings for both capital and operational expenses.

4.2.1.2 Operational Cost Considerations

In order to run a basic EC3, supporting multiple PSAPs at a State or sub-State Regional level in a 24x7 capacity, the minimum amount of staff needed to do so is projected at five analysts and one manager. The manager should also act as a person-on-call so that issues after hours may be escalated as needed. As the operation grows and additional staffing is required, the operation can then add more people to the busier shifts.

As a general rule of thumb, WG1 has updates some previous estimates to err on the high side of possible costs. Keeping in mind that these costs, like capital costs, vary widely depending on location, the WG believes that obtaining individuals with the education and experience needed to fulfill these roles will cost from between $125,000 and $200,000 per year per person. Using an average cost per employee of $162,500 the ***very rough estimate*** as to operational, recurring costs to operate a small to medium EC3 will be approximately $812,500 per year. Cost for benefits for these personnel range from between 18 to 30 percent on a nationwide average. Using a blended average of 24 percent, the approximate **personnel costs only** of the center would be **$1,007,500.** A center requiring twice as many personnel, would incur twice as much cost.

While it is not possible to definitively predict the cost for every individual EC3, as there are a number a variables, this average assumes one center that supports multiple PSAPs and is staffed 24 hours a day, 365 days a year. Larger centers, supporting larger geographic areas or in need of greater data capabilities and personnel will obviously incur additional cost. The suggested estimate is intended to provide a guideline, not a quote, to enable PSAPs and 9-1-1 Authorities to gauge potential cost sharing, and cost saving, options and make informed decisions.

In addition to the personnel expenses, there will be costs for utilities, bandwidth, and communications, the need for sensors, potential annual costs for those elements, as well as recurring rent or taxes. WG1 has attempted to “drill down” a bit farther into some specific costs and has asked current industry partners to provide some high level estimates of potential associated costs.

Thanks to input from one such provider, Table 3 provides a breakdown of a typical monthly service cost, based on the throughput of the network’s Internet connection to be monitored. This information is provided for base reference purposes only and the working group is not suggesting, or endorsing, any specific product or product suite.

Table 3 – Internet Provisioning Costs

Pricing: ▪ Based on Internet Provisioned Connection Size. ▪ One-time initiation fee of **$850, per sensor**	
Internet Connection Size	**Cost per month**
Size up to 10MB	**$590**
Size > 10MB-100MB	**$890**
Size > 100MB-1GB	**$1,390**
Size > 1GB - 10GB	**$2,790**

Again, based on high level information provided by an existing service provider in this space, a number of additional options for inclusion on the EC3 model exist. Included among these options is a managed security services approach. This system is comprised of monitoring and/or management of security devices to include:

- Security Event Analysis & Notifications 24x7
- Monitoring and Management services are available for the following security devices. Firewall monitoring
- Host-based Intrusion Detection System monitoring
- IDS/IPS monitoring and management
- Proxy monitoring

In addition to these services, other assessment services may be offered. These include network assessment services, described at a high level in Table 4, and web application assessment, as described in Table 5. These are generic in the sense that no specific customer or application is named, however they provide some additional granularity into the additional services likely required to support EC3 activities and the additional costs associated with those services.

Table 4 - Network Assessment Services

Annual cost per Live IP Scanned			
Service Level Based on the Number of Live IPs Scanned per period per Reporting Entity	**One Time Assessment**	**Quarterly Assessments**	**Monthly Assessments**
10	$88	$120	$189
16-25	$67	$92	$151

Annual cost per Live IP Scanned			
Service Level Based on the Number of Live IPs Scanned per period per Reporting Entity	**One Time Assessment**	**Quarterly Assessments**	**Monthly Assessments**
26-50	$55	$75	$128
51-100	$44	$59	$105
101-200	$26	$38	$77
201-500	$22	$32	$65
501-2,000	$19	$27	$53

Table 5 - Web Application Assessment

Annual Cost per Web App Scanned			
	One Time Assessment	**Quarterly Assessments**	**Monthly Assessments**
First Web App per Entity	$1,025	$1,322	$1,918
Additional Web App per Entity	$569	$867	$1,463

In addition to the potential costs noted above, some organizations have proposed a membership based approach, which establishes annual costs based on the size of the organization wishing to subscribe. As described in Table 6, membership fees are based on the total number of people employed at an organization.

Table 6 – Annual Membership Fee for Web Application Assessment

Organization Employee Range	**1-Year Membership Cost**	**2-Year Membership Cost**	**3-Year Membership Cost**
250,000 or more	$9,926	$ 19,852	$ 29,778
100,000 to 249,999	$9,191	$ 18,382	$ 27,573
50,000 to 99,999	$8,456	$ 16,912	$ 25,368
25,000 to 49,999	$7,721	$ 15,442	$ 23,163
10,000 to 24,999	$7,350	$ 14,700	$22,050
5,000 to 9,999	$6,986	$13,972	$20,958
1,000 to 4,999	$6,615	$13,230	$19,845

Organization Employee Range	1-Year Membership Cost	2-Year Membership Cost	3-Year Membership Cost
500 to 999	$4,781	$9,562	$14,343
250 to 499	$3,311	$6,622	$9,933
100 to 249	$2,394	$4,788	$7,182
50 to 99	$1,470	$2,940	$4,410
Up to 49	$924	$1,848	$2,772

Taking each of these potential services into account, Table 7 provides a total rough estimate of the annual operating cost of small to medium EC3 and medium to large EC3.

Table 7 - Total Rough Estimate of Annual Operating Expenses

Operating Expense	Small to Medium EC3		Medium to Large EC3	
	Annual Cost	Assumption	Annual Cost	Assumption
Employee Expenses	$1,007,500.00	Projected five analysts and one manager 24% cost for benefits	$2,015,000.00	Projected five analysts and one manager 24% cost for benefits
Internet Provisioning	$33,480.00	1GB to 10GB per month, at a cost of $2,790/month	$33,480.00	1GB to 10GB per month, at a cost of $2,790/month
Live IP Scanning	$15,400.00	Assumes $77/ month/IP scanned using the number of 200 IPs scanned	$106,000.00	Assumes $53/month, or 2000 IPs scanned
Web Application Assessment	$40,572.00	$3,381/month	$216,132.00	$18,011/month assuming 1 new, and 10 additional Web Applications evaluated each month
Web App Membership Cost (optional)	*$2,394.00*	*1 year Membership Costs for organization size of 100 to 249*	*$4,781.00*	*For an organization with up to 999 members*
Utilities, Bandwidth, and Communications; Annual Rent; Taxes	$200,000.00	Average cost, but these costs can vary widely depending on the location of the center, the types of technologies chosen, and the amount of bandwidth required	$200,000.00	Average cost, but these costs can vary widely depending on the location of the center, the types of technologies chosen, and the amount of bandwidth required
Total	**$1,299,346.00**		**$2,575,393.00**	

The rough estimate for operational expenses of a small to medium EC3, supporting multiple small or medium sized PSAPs would be $1,299,346 per year. Using the same logic, a larger center, capable of supporting multiple medium to large PSAPs, with a great deal more traffic and real time scanning and analysis requirements, would be approximately $2,575,393 per year. This assumes a center with twice as many personnel as the small/medium EC3.

4.2.1.3 Summary of Cost Considerations

As shown, there are substantial costs associated with building out the physical and network related architectures and operating and maintaining the systems that will support cybersecurity functions. Rather than suggesting that each of the more than 6,000 PSAPs in the United States be burdened with building and staffing such facilities, the working group believes utilizing core EC3's at various levels (Regions within a State, State level, or Regions comprised of multiple States and 9-1-1 authorities) can offer public safety both economies of scale and operational efficiencies. In addition, a cooperative approach on the cybersecurity front brings a greater number of resources to bear for any incident, provides small, medium, and large PSAPs with equal resources and capabilities to defend against, and recover from, cyber-attacks and allows for real time information sharing and intelligence. In addition, monitoring systems that are respectful of PII, such as those mentioned previously, will allow for the sharing of network and system health without compromising the security of individuals or organizations.

WG1 would like to stress regardless of estimated personnel costs, we believe identifying, hiring and especially retaining adequate professional staff in this area of expertise will be challenging to do at an individual PSAP or 9-1-1 authority level. The demand for these trained professionals is very high. This is another example of why a cooperative approach, and utilizing core services for deployed (PSAP) customers becomes both more practical and more manageable.

5 Information Sharing Environments

The importance of information sharing cannot be understated. In the current environment, PSAPs perform multiple critical functions for their jurisdictions. Many of these functions are common across all lines of operation and regardless of locality. However, the ability to share information in real time, between multiple PSAPs, agencies, and jurisdictions has not been refined. As part of the overall approach to cybersecurity, it is crucial that PSAPs, 9-1-1 Authorities, and the agencies they all support, are able to share intelligence in a real time, or near real time environment.

While we have not yet made the transition to all IP networks and systems, the opportunity exists today to participate in a number of information sharing enviroments (ISEs) which are designed to share data, best practices, and resources amongst multiple elements within the public safety community. To date, many of these remain underutilized. The intent of this section of the report is to highlight, and provide links to, a number of ISEs that exist and should be considered by public safety and emergency communications partners.

Membership and/or participation in these ISEs comes at little or no cost to the agency. As a result, the significant return on investment, in the form of increased information sharing, situational awareness, and actionable intelligence, is quite valuable to any agency or organization that participates. Any or all of the options presented below are available partners in the cybersecurity space for FSLTT PSAPs, 9-1-1 Authorities, and responder agencies. WG1 encourages agencies to become familiar with these options and to engage in information sharing with multiple partners sooner rather than later.

5.1 The Office of the Director of National Intelligence (ODNI)

The Office of the Director of National Intelligence offers a number of ISEs and programs in which public safety and emergency communications entities can participate. Additionally, there are opportunities for public safety to expand their role, and thus the level of inter-agency communications, via several of these mechanisms. The following figure illustrates a high level vision of information sharing and interoperability based on the ISE model.

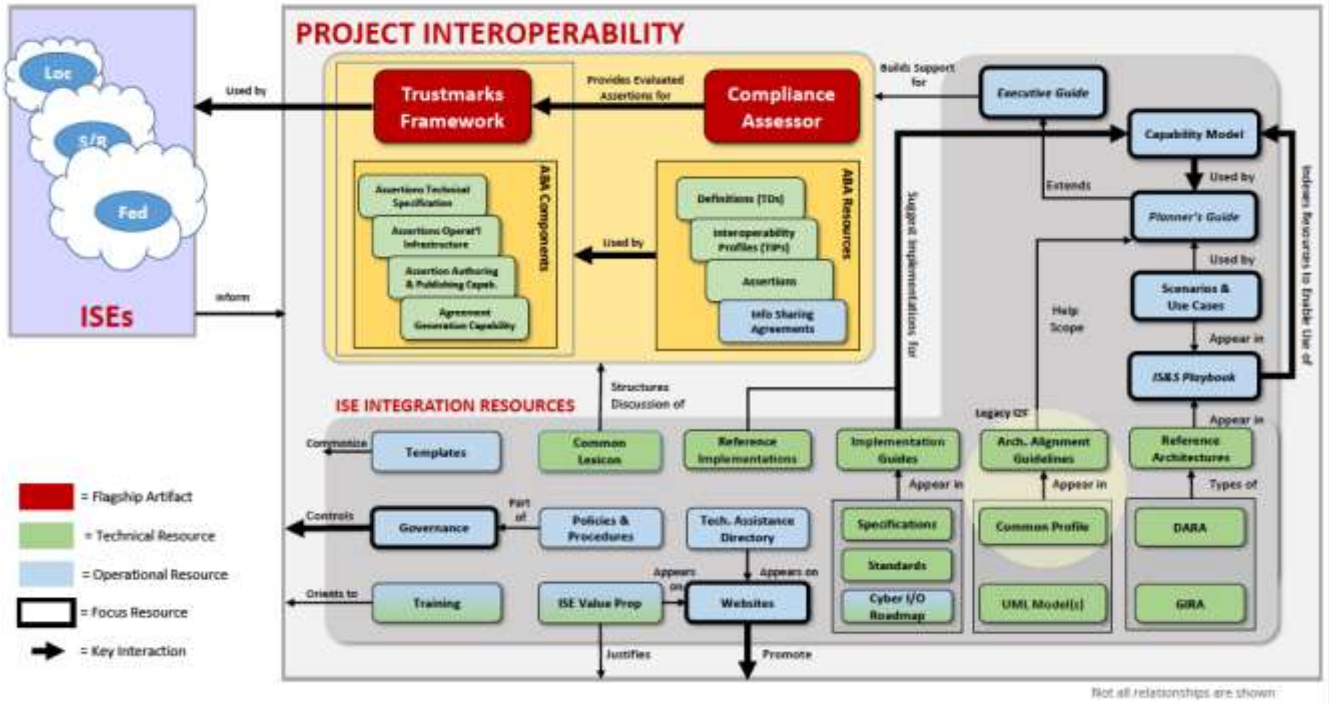


Figure 3 - ODNI Project Interoperability

5.1.1 What Is The ISE?

The Information Sharing Environment (ISE) broadly refers to the people, projects, systems, and agencies that enable responsible information sharing for national security.

This includes many different communities: **law enforcement, public safety**, **homeland security**, **intelligence**, **defense**, and **foreign affairs**. While they work in different disciplines and have varying roles and responsibilities, members of these communities all rely on timely and accurate information to achieve their national security mission responsibilities.

Although the nature is unclassified, Sensitive but Unclassified (SBU) information is a cornerstone for decision making across ISE communities. The goal is to enable **Federal**, **State**, **Local**, and **Tribal** ISE communities to share SBU information regardless of who owns the underlying systems or information. To become a member and share or exchange SBU information, please visit **www.ise.gov** for additional information. WG1 has included a number of links to various ISE sources in Appendix A of this document.

5.2 Department of Homeland Security

DHS offers a collection of programs and initiatives that can be applied to reduce NG9-1-1 cyber risks. Many of these efforts support approved missions that cover FSLTT users, as well as public and private critical infrastructure entities. Appendix B details a number of these programs, designed to foster information sharing and situational awareness.

DHS also relies heavily on voluntary collaboration with its partners. Working closely with those federal departments and agencies most responsible for securing the government's cyber and communications systems, and actively engaging with private sector companies and institutions, SLTT governments, and international counterparts DHS hopes to foster information sharing at all levels. Each group of stakeholders represents a community of practice, working together to protect the portions of critical information technology that they own, operate, manage, or interact with. PSAPs, 9-1-1 Authorities, and major public safety associations such as APCO and NENA all have an opportunity to be represented, and participate in, multiple programs under the DHS umbrella. As with the other information sharing environments, the DHS programs listed in Appendix B represent an opportunity for public safety to engage in information sharing, and gain both proactive and reactive assistance with regard to cyber threats.

5.3 Information Sharing and Analysis Organizations (ISAOs)

ISAOs are a new take on information sharing for communities of practice. Many agencies have found it challenging to develop effective information sharing organizations. In 2015 President Obama issued Executive Order 13691 directing DHS to encourage the development of ISAOs. Our cyber adversaries move with speed and stealth and have been proven to oupace our efforts to thwart them in many instances. While many critical infrastructures can find representation in the existing Information Sharing Advisory Council (ISAC) structure, those beyond traditional critical infrastructure sectors also need to be able to share information and respond to cyber risk in as close to real-time as possible. Organizations engaged in information sharing related to cybersecurity risks and incidents play an invaluable role in the collective cybersecurity of the United States.

Overview

Executive Order 13691, Promoting Private Sector Cybersecurity Information Sharing, directs DHS to:

- Develop a more efficient means for granting clearances to private sector individuals who are members of an ISAO via a designated critical infrastructure protection program;

- Engage in continuous, collaborative, and inclusive coordination with ISAOs via the NCCIC, which coordinates cybersecurity information sharing and analysis amongst the Federal Government and private sector partners; and

- Select, through an open and competitive process, a non-governmental organization to serve as the ISAO Standards Organization. This ISAO Standards Organization will identify a set of voluntary standards or guidelines for the creation and functioning of ISAOs.

Expanding the Current Model

Currently, most private sector information sharing is conducted through Information Sharing and Analysis Centers (ISACs). ISACs operate through a sector based model, meaning that organizations within a certain sector (i.e. financial services, energy, aviation, etc.) join together to share information about cyber threats. Although many of these groups are already essential drivers of effective cybersecurity collaboration, 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 cyber threat information could benefit from membership in an ISAO.[2]

6 Identity Credentialing Access Management (ICAM)

There are internal and external risks to NG911 cybersecurity associated with ICAM. ICAM refers to intersections of digital identities and associated attributes, credentials and access controls into one comprehensive approach, as would be needed to minimize internal threats, both manmade intentional and manmade unintentional. If identity management solutions are not properly implemented as part of NG911 services, then NG911 will be vulnerable to internal attackers with limited attribution, and more vulnerable to accidental acts that disrupt services in a manner which may be undetected longer due to its unintentional nature.

Externally, traditional methods to identify and locate the end user will change as some scenarios will be entirely digital and cyber attackers may employ methods to mask, alter, or corrupt physical location(s) and digital content they provide to the PSAP. Examples of these risks have already been seen in 9-1-1 systems around the country, in the forms of "SWATTING" and spoofing[3]. In traditional 9-1-1 service, the operator may be able to detect (through human interaction) attempts to misuse 9-1-1 services, and PSTN phone number tracing can help to validate end user location and identify.

NG911 must balance the need for end user identification, access, and credentialing associated with IP calling and text messaging, with operational requirements to respond rapidly and provide universal access to 9-1-1. In NG911, these elements change. ICAM matters present new shared risks and risk mitigations that PSAP operators and telecommunications service providers should address together. There are proven methods that can reduce risk, such as identity and access controls and capabilities to geolocate the user. Interactions in NG911, in many cases, will not contain the same level of human interaction that was part of virtually all traditional 9-1-1 operations. Dialogues may be only digital, and to ESInet, an attacker end point will likely look identical to an end point behind which a human is seeking help for a real world emergency.

Key ICAM Service Areas for consideration by PSAP and 9-1-1 Authorities include:

- Digital Identity
- Credentialing

[2] https://www.isao.org/faq/

[3] SWATTING is a reference to pranksters manipulating IP-based 9-1-1 calls to indicate the call is originating from a location at which a most serious criminal act has taken or is taking place, such as armed and violent hostage takers or similar situations so significant that the local PSAP dispatches a Special Weapons and Tactics (SWAT) team to the address. Spoofing is similar, in that emergency calls are placed from one IP address which has been manipulated to appear to be sent from another. Spoofing is generally done to create annoyances and have less potential risk to the occupants at the spoofed location than a false call which results in a SWAT team deployment.

- Privilege Management
- Authentication
- Authorization & Access
- Cryptography
- Auditing and Reporting

ICAM Drivers

Cybersecurity threats continue to increase. At present, there is no National, or International, Industry "standard" approach to individual identity on the network. While some Federal initiatives are underway, such as the National Strategy for Trusted Identies in Cyberspace (NSTIC)[4], an actual standard, or set of standards, which would be both applicable and acceptable to local public safety entities is still lacking. Security weaknesses include the areas of user identification and authentication, encryption of sensitive data, logging and auditing, and physical access. In addition, there is a demonstrated need for improved physical security, a lag in providing government services electronically, clearly identified vulnerability of Personally Identifiable Information (PII) and a lack of interoperability.

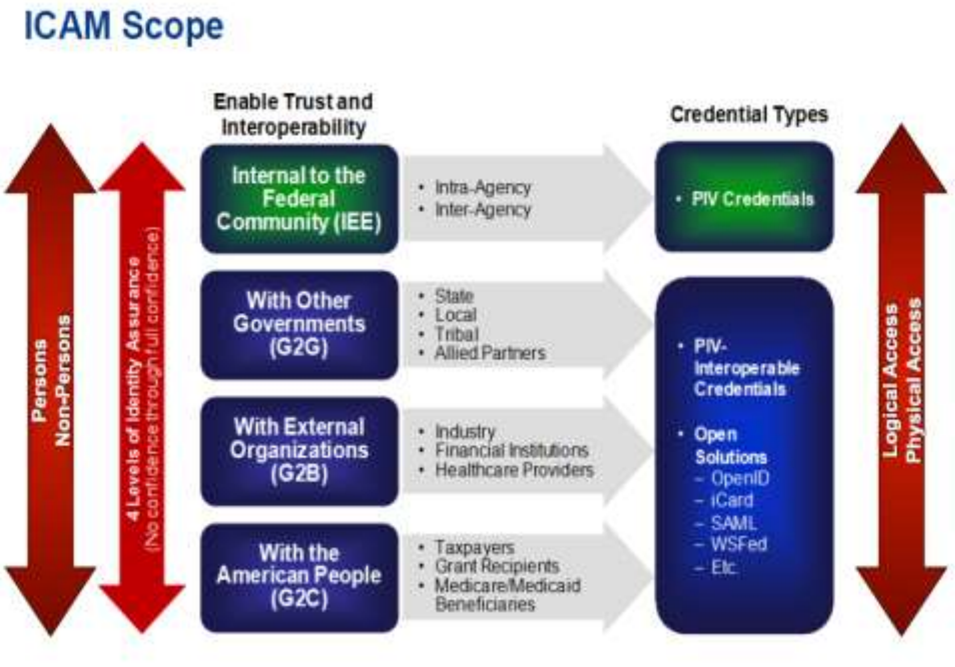

ICAM Scope
Enable Trust and Interoperability
Credential Types
Persons
Non-Persons
4 Levels of Identity Assurance
(No confidence through full confidence)
Internal to the Federal Community (IEE)
• Intra-Agency
• Inter-Agency
• PIV Credentials
With Other Governments (G2G)
• State
• Local
• Tribal
• Allied Partners
With External Organizations (G2B)
• Industry
• Financial Institutions
• Healthcare Providers
With the American People (G2C)
• Taxpayers
• Grant Recipients
• Medicare/Medicaid Beneficiaries
• PIV-Interoperable Credentials
• Open Solutions
– OpenID
– iCard
– SAML
– WSFed
– Etc
Logical Access
Physical Access

Figure 4 - ICAM Scope

M-04-04[5] and NIST 800-63-2[6] are still the foundational policy/technical guidance for

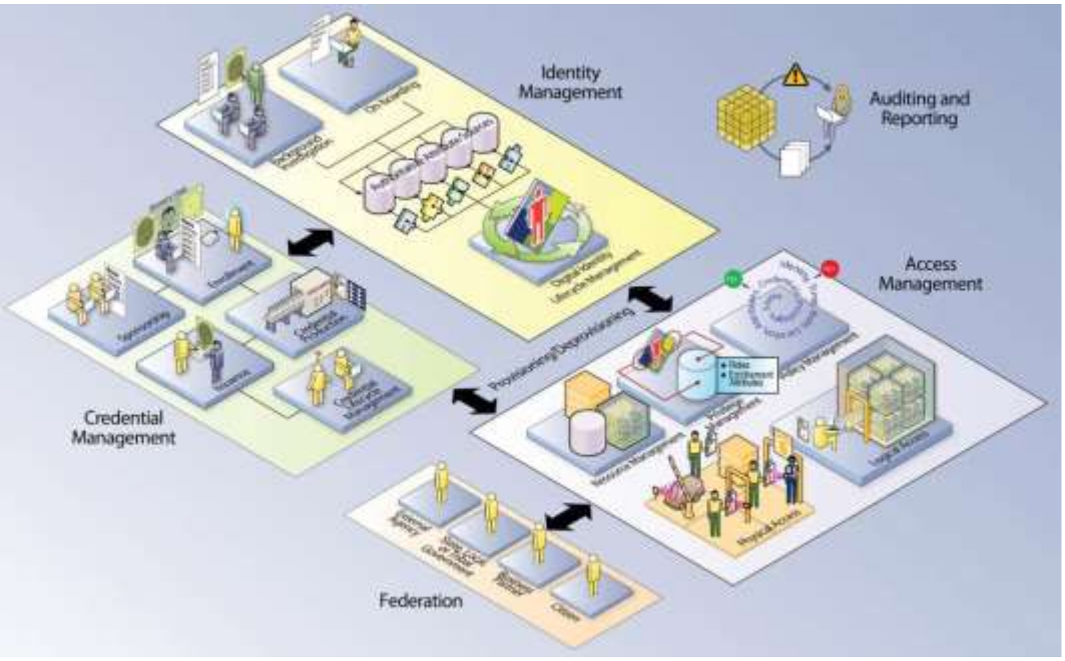
[4] https://www.nist.gov/itl/tig

[5] https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf

identity management in the Federal government. These documents can also be used as a starting point for SLTT agencies and organizations. At a basic level, there is a need for any agency that will eventually interconnect into a larger information sharing environment, and or EC3 service, to do each of the following:[7]

- Establish unified architecture for Identity Management
- Conduct outreach to communities of interest within the SLTT spectrum
- Increase the community of trust through innovative interfederation at all levels of assurance
- Promote strong credential usage (Tokens, PKIs, PIV, etc)
- Establish partnerships with industry providers
- Establish agreed upon Profiles for open identity solutions
- Establish Trust Framework Provider(s)
- Establish Privacy Principles

Identity and Access Management are Foundational to information sharing and collaboration. The intent of the ICAM discussion in this report is not to suggest that local, regional, state or tribal agencies be required to utilize any type of single user, single sign-on approach. Rather, the intent is to provide an education as to the need for identity control and access management at all levels of interface.



[6] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf

[7] http://www.internet2.edu/presentations/spring10/20100427-gsa-pencer.pdf

Figure 5 - ICAM - The Big Picture

When properly aligned, ICAM creates a basis for trust in securely enabling electronic transactions, which should include secure access to facilities and installations. Just as identity, credential, and access management activities are not always self-contained and must be treated as a cross-disciplinary effort, ICAM also intersects with many other IT, security, and information sharing endeavors.

7 Recommendations

7.1 Near-Term

Recommendation #1: Provide a funded pilot for the development and deployment of an EC3 including Network and Wireless / Wireline sensors and IDPS functionality.

In order to identify the challenges and qualify the benefits associated with deployment, the build out of a single EC3 in targeted region or specific PSAP is recommended. This pilot should demonstrate the planning, requirements gathering, design, implementation and maintenance considerations of deploying an EC3. The pilot should also be designed to provide proof-of-concept that the sensor alerts can be correlated into actionable data and integrated into mitigation solutions.

Recommendation #2: Encourage public safety communications community to learn about and participate in Information Sharing Environments.

This effort may include outreach activities and a study of current challenges and barriers to ISE participation. Legal, regulatory, privacy, and technical barriers exist to the efficient and effective sharing of cybersecurity events.

Recommendation #3: Support research into additional capabilities for integration with the EC3 model.

Some additional capabilities are addressed in the Operational Cost Considerations section of this document, but potential capabilities must be balanced with performance considerations, impact to operational procedures, and funding considerations. Out year costs subsequent to the deployment and initial operations need definition as governing authorities of local, county, State and Tribal entities will have to have comprehensive costing and sustainment information if they are to embrace this offering. Sources of additional funding for capital and O&M sustainment along with potentials to cost share and model to do so would also be important financial considerations.

Recommendation #4: Investigate additional network and wireless carrier sensor implementations for alternate technologies, best practices and lessons learned.

Ongoing research projects and various commercial cybersecurity innovations monitoring voice and data networks may prove to have valuable information regarding the expectations and challenges encountered by the public safety community in implementation.

Recommendation #5: Encourage 9-1-1 Authorities to inventory their systems and participate in Critical Infrastructure Cyber Community Voluntary Program.

As part of Executive Order (EO) 13636 DHS launched the Critical Infrastructure Cyber Community or C³ (pronounced "C Cubed") Voluntary Program to assist the enhancement of critical infrastructure cybersecurity and to encourage the adoption of the NIST Cybersecurity Framework (the Framework), released in February 2014. The C³ Voluntary Program was created to help improve the resiliency of critical infrastructure's cybersecurity systems by supporting and promoting the use of the Framework.

Recommendation #6: Encourage 9-1-1 Authorities to investigate and discover programs mentioned in this and the original TFOPA reports within their regions.

Many of these programs are known of or cursory understood but where and how to best utilize them at the local level is not known.

7.2 Mid-Term

Recommendation #7: Develop a comprehensive plan or a roadmap, for build out of EC3 and/or cybersecurity core to protect NG9-1-1 core services.

This comprehensive plan would address the end user requirements and key performance indicators of such a system. Employing an RFI to determine potential architecture options may be advisable. Full lifecycle planning for cyber risk mitigation should include governance, technology, usage, security, standard operating procedures and training and exercises to address:

- Identification of new and evolving risks
- Assessment and prioritization of risks
- Development and prioritization of mitigation strategies based on cost-benefit analysis and other factors
- Evaluation the impacts of mitigation implementation
- Evaluations and development of transitional architectures for migratuion of 911 PSAPs from basic, E911,limited NG911 features to end state NG911 deployments delineating the cyberdefense/cyber mitigation characteristics and capabilities within these transitions amd migrations.
- Development of an approach to detection and effective response and recovery procedures, including standardized information sharing practices
- Decommissing of legacy infrastructure/services/applications
- Research, development and innovation efforts to achieve maximum ROI on investment

The federal responsibilities should be clearly defined for any national-level assets, and standaridized interconnection guidance (e.g., policies, best practices, operational procedures) must be made available for the various models of implementation. Various operational models should include how PSAPs join EC3s, interconnection policies, shared responsibilities, shared costs, security policy, system change notification requirements, and service level agreements.

Recommendation #8: Provide a gap analysis on the currently available capabilities and the ideal state of deployment at a national level (supportive of local control and enabled through state-level coordination).

There are various limitations of the current potential implementations, such as the challenges in finding and retaining skilled staff, vetting products/vendors, resiliency and survivability of implementations, inconsistencies in service offerings (between EC3s), liability, privacy and the fact that only attacks with an Internet-based component will be identified. Providing an analysis of limitations will allow stakeholders to focus on finding solutions or accepting the risk of various challengs.

Recommendation #9: Require carriers, vendors and application developers to participate in cybersecurity best practices when interfacing with NG911and other PSAP/PSCC systems.

With vast NG911 interconnection possibilities, it will be difficult to discern if local, state, tribal or Federal authorities can or should apply cybersecurity standards to satisfy mandates from their own governments to systems for which they have not contributed funds, hold no direct authority, or provide other resources to support beyond network access and perhaps mutual aid agreements—even if they share redundancies, databases, or other resources. To this end, potential vendors of NG911 services that will interface with NG911, or other PSAP/PSCC systems should be responsible for employing cybersecurity best practices, as required by the local or State organizations. These requirements can clearly be spelled out in RFP's and could also potentially be tied to any federal funding for the construct and implementation of an NG911 system. Clearly defining cybersecurity requirements at the onset will allpow public safety to deploy protected systems rather than having to retroactively protect already deployed systems.

7.3 Long-Term

Recommendation #10: Complete build out and deployment of EC3s on national level and interconnect all PSAPs, PSCCs, EOCs, and potentially FirstNet.

While executing on the comprehensive plan defined in Recommendation #5, this recommendation could be supported by development of NG911-specific policy related to cybersecurity; creation of best practices, standards, and defined requirements for EC3 implementation and operational models; and continued outreach to the public safety community regarding EC3 benefits.

8 Follow On Work

The Working Group recognizes that the local control is essential to any public safety related project at the State, local and tribal levels, and an architecture, or architecture options, balanced with the need to create a manageable core infrastructure which supports distributed network elements to the PSAP level is equally important. Recognizing the importance of delving further into multiple issues, WG1 believes that there is important follow on work that should be conducted by either the next iteration of TFOPA, or a related group.

Regular communications to local, state, tribal and regional 9-1-1 authority levels for updates and further involvement or awareness of federal systems and programs regarding Cyber Security and Cyber hygiene should become the norm, not the exception. Further study, and reporting, into the use of existing mechanisms for information sharing, such as those detailed in this report, should be conducted. In addition, pilot programs incorporating PSAPs, 9-1-1 Authorities, and the public safety communications sector in general, should be considered.

Development and maintenance of a list of programs to be considered by PSAPs and 9-1-1 Authorities for for the purposes of Cyber Security within their PSAP jurisdictions could be considered. This list could be hosted by either DHS or the FCC. Federal programs with 9-1-1 related Cyber Security functions could also be listed with contact information or instructions on how to participate.

Through our presentations and discussions it became more apparent that data analytics will be a major component of a Cyber Security solution and should not be underestimated. From a standpoint of sizing capacity for data collection, as well as weeding through the mass of data that will be collected to identify real and potential threats from the false positives, there is more study and work to be done on this front. Future work might include an analysis of the types, and potential amounts, of such data and what current solutions might exist to meet these needs at various levels.

While not a specific task of WG1, continued research and development of workforce training strategies and approaches is extremely important. As noted in the first TFOPA report, our personnel are our most valuable asset. Training, awareness, and ongoing education of personnel with regard to cyber hygiene and sound cybersecurity practices is essential.

It is recommended that appropriate agencies (e.g.- DOJ, DHS, NSA) should explore options for sharing data, derived from classified reporting. In an operational environment, real time, or near real time, intelligence is critical to responder safety and public welfare. Understanding that classification exists for good reason, and with no intent of circumventing normal channels, the WG suggests that further study into possible mechanisms for sharing this information with public safety may be warranted.

Finally, WG1 recognizes that privacy issues which will be of concern to public safety and the public alike. As with any other area of cybersecurity, privacy must remain a key factor in how a solution is engineered and implemented. WG1 suggests that additional research into this area would be a productive endeavor.

9 Conclusion

The working group believes that a lack of attention to cybersecurity continues to pose a clear and present danger to the PSAP and public safety communications system(s) in the United States. The recent TDoS attacks targeting 9-1-1, continuing probing attacks against communications infrastructure, and the availability of hacking as a service all add to these concerns.

It is more critical than ever that agencies at all levels of government begin the process of analyzing and defending their public safety networks and systems from all manner of cyber attack. Creation of some core services, which provide single points of contact, direct reporting, awareness, and data sharing, and real time response to cyber attacks at multiple levels of government is essential to the success of these efforts. While the actors, vectors, and outcomes for cyber attacks against public safety continue to vary widely, the approach public safety takes to defending this domain must be targeted, cooperative, collaborative and resolute.

Monitoring of the networks that feed the 9-1-1 system, and of the data systems within and between PSAPs, is of great importance. The deployment of different types of sensors is also a recommendation that WG1 made in its initial report, that will benefit the entire public safety enterprise. The correlation of data across multiple partners and tracking, and sharing, of data as to how threats evolve as they begin to affect the various SLTT entities being monitored is also crucial.

This report provides some additional high level estimates of potential costs. As stated, there are a number of variables that must be taken into account and sizing of an EC3, or cyber defense plan, will depend largely upon local requirements and needs. However, WG1 continues to emphasize that sharing of core infrastructure as it relates to cybersecurity is an effective way to mitigate costs, expand capabilities, and share critical information in real time with public safety partner agencies. To this end, the deployment of EC3, or EC3 like, systems should be a collaborative effort between Federal, State, Local, Tribal and Territorial partners.

WG1 has suggested additional follow on work from which public safety communications would benefit, and made recommendations for funded pilot programs to “kick start” the EC3 design, deployment, and implementation effort. The WG strongly believes that beginning these efforts sooner rather than later will benefit the entire Nation.

Finally, WG1 and its members would like to take this opportunity to thank the FCC and the FCC’s Public Safety and Homeland Security Bureau (PSHSB). Without the future looking vision of the FCC and PSHSB in forming TFOPA, and without their leadership, guidance, and support, none of this work would have been possible. As public safety communications professionals from both the public and private sectors, WG1 members are grateful for the opportunity to have participated in the TFOPA work. It is our sincere hope that this work will assist public safety agencies and entities across the United States in understanding and preparing for cybersecurity needs now and in the future.

APPENDIX A- ODNI Information Sharing Resources

- SENSITIVE BUT UNCLASSIFIED (SBU): OVERCOMING BARRIERS TO FEDERATE INFORMATION SHARING ENVIRONMENTS
  https://www.ise.gov/mission-stories/standards-and-interoperability/sensitive-unclassified-sbu-overcoming-barriers

- SECURITY TRIMMED FEDERATED SEARCH: GETTING THE RIGHT INFORMATION TO THE RIGHT PEOPLE AT THE RIGHT TIME
  https://www.ise.gov/mission-stories/security-trimmed-federated-search

- PROJECT INTEROPERABILITY: BUILDING A FOUNDATION OF TECHNOLOGICAL COLLABORATION TO SUPPORT TERRORISM-RELATED INFORMATION SHARING
  https://www.ise.gov/mission-stories/standards-and-interoperability/project-interoperability-building-foundation

- ESTABLISHING TRUST AND INTEROPERABILITY IN THE INFORMATION SHARING ENVIRONMENT
  https://www.ise.gov/mission-stories/standards-and-interoperability/establishing-trust-and-interoperability-information

- GEOSPATIAL ENHANCEMENT FOR NIEM EFFORT (GEO4NIEM)
  https://www.ise.gov/mission-stories/geo4niem

- FY16 INFORMATION SHARING INITIATIVE HIGHLIGHTS FOR STATE AND LOCAL LAW ENFORCEMENT
  https://www.ise.gov/mission-stories/fy16-information-sharing-initiative-highlights-state-and-local-law-enforcement

- SUPPORTING CRISIS COMMUNICATIONS
  https://www.ise.gov/mission-stories/communications-and-partnerships-governance-standards-and-interoperability/supporting

Links to Program manager – information sharing environment mission stories

<u>MISSION FOCUS AREA: *CYBER*</u>

- DEFINING AND FIGHTING CYBER TERRORISM IN AN INCREASINGLY COMPLEX LANDSCAPE
  https://www.ise.gov/mission-stories/defining-and-fighting-cyber-terrorism-increasingly-complex-landscape

- STRENGTHENING NATIONWIDE CYBER CRIME FIGHTING CAPABILITIES
  https://www.ise.gov/mission-stories/communications-and-partnerships/strengthening-

nationwide-cyber-crime-fighting

- DATA AGGREGATION REFERENCE ARCHITECTURE IMPLEMENTATION
https://www.ise.gov/mission-stories/governance-standards-and-interoperability/data-aggregation-reference-architecture

- CYBER INTELLIGENCE NETWORK: FACILITATING THE RAPID EXCHANGE OF CYBER INTELLIGENCE
https://www.ise.gov/mission-stories/communications-and-partnerships-governance-standards-and-interoperability/cyber

- MALWARE INVESTIGATOR: CONNECTING THE DOTS
https://www.ise.gov/mission-stories/communications-and-partnerships-governance-standards-and-interoperability/malware

- FUSION CENTERS COLLABORATE TO SUPPORT ARREST OF INDIVIDUAL CHARGED WITH PRODUCTION OF CHILD PORNOGRAPHY
https://www.ise.gov/mission-stories/communications-and-partnerships/fusion-centers-collaborate-support-arrest-individual

MISSION FOCUS AREA: *DOMAIN AWARENESS*

- GEOSPATIAL ENHANCEMENT FOR NIEM EFFORT (GEO4NIEM)
https://www.ise.gov/mission-stories/geo4niem

- SUPPORTING CRISIS COMMUNICATIONS
https://www.ise.gov/mission-stories/communications-and-partnerships-governance-standards-and-interoperability/supporting

- SECURITY TRIMMED FEDERATED SEARCH: GETTING THE RIGHT INFORMATION TO THE RIGHT PEOPLE AT THE RIGHT TIME
https://www.ise.gov/mission-stories/security-trimmed-federated-search

- BRINGING TOGETHER KEY STAKEHOLDERS IN WASHINGTON STATE'S PUGET SOUND
https://www.ise.gov/mission-stories/puget-sound-interoperability

- ACHIEVING MARITIME DOMAIN AWARENESS: GOVERNMENT WORKING TO RELEASE ARCHITECTURE PLAN AND FUNCTIONAL STANDARD
https://www.ise.gov/mission-stories/maritime-domain-awareness-plan

MISSION FOCUS AREA: *STATE AND REGIONAL*

- PROJECT INTEROPERABILITY: BUILDING A FOUNDATION OF TECHNOLOGICAL COLLABORATION TO SUPPORT TERRORISM-RELATED INFORMATION SHARING
https://www.ise.gov/mission-stories/standards-and-interoperability/project-

interoperability-building-foundation

- ESTABLISHING TRUST AND INTEROPERABILITY IN THE INFORMATION SHARING ENVIRONMENT https://www.ise.gov/mission-stories/standards-and-interoperability/establishing-trust-and-interoperability-information

- MEASURES OF SUCCESS: PILOTING A CULTURE OF METRICS REPORTING IN THE INFORMATION SHARING ENVIRONMENT https://www.ise.gov/mission-stories/governance/measures-success-piloting-culture-metrics-reporting-information-sharing

- COUNTERING VIOLENT EXTREMISM: INFORMATION SHARING HIGHLIGHTS FROM THE DENVER INTERVENTION PILOT https://www.ise.gov/mission-stories/countering-violent-extremism-information-sharing-highlights-denver-intervention

- FY16 INFORMATION SHARING INITIATIVE HIGHLIGHTS FOR STATE AND LOCAL LAW ENFORCEMENT https://www.ise.gov/mission-stories/fy16-information-sharing-initiative-highlights-state-and-local-law-enforcement

MISSION FOCUS AREA: *WATCHLISTING, SCREENING, AND ENCOUNTERS*

- SENSITIVE BUT UNCLASSIFIED (SBU): OVERCOMING BARRIERS TO FEDERATE INFORMATION SHARING ENVIRONMENTS https://www.ise.gov/mission-stories/standards-and-interoperability/sensitive-unclassified-sbu-overcoming-barriers

Program Manager – Information Sharing Environment Portfolio Summary

State and Regional Information Sharing Environments

The State and Regional ISE portfolio supports all 50 states and geographic regions seeking to actively increase information sharing between and among themselves and federal partners. The portfolio is especially focused on assisting those pursuing the creation of Information Sharing Environments by developing and providing governance and management guidance as well as tailored sets of interoperability tools.

Goal: Increase efficiency of request for, discovery and access to, and use of threat-related data among and between State, Regional, Local, and Federal partners, both within and outside of the National Network of Fusion Centers and the Criminal Intelligence Coordinating Council (CICC).

Law Enforcement Identity Vetting

Creation of a secure web-based registration site for government-wide law enforcement officers to be vetted and approved for access to ISE-related SBU networks and resources.

Partners: DOJ, BJA, IIR, RISS, and Department of Homeland Security (DHS), Georgia Tech Research Institute (GTRI).

Real-time Open Source Analysis (ROSA) Toolkit

Develop a ROSA Toolkit for law enforcement agencies to identify resources and guidance documents to assist in the development of a ROSA process.

Partners: IIR, Northern California Regional Intelligence Center (NCRIC), RISS, Central Florida Intelligence Exchange, New Jersey Urban Areas Security Initiative

National Fusion Center Association (NFCA) Engagement

Participation and support through subject matter expertise to the NFCA's workgroups and sub-committees. Current support to the Social Media Workgroup has developed goals and deliverables, to support a toolbox for delivery in September of this year to be used by state and local law enforcement. Support to the NFCA sub-committees advance such aspects as technology, private sector engagement, and cyber security and investigations. Support to these groups will continue to add value to national security.

Criminal Intelligence Coordination Council (CICC) Engagement

Part of DOJ's Global Justice Information Sharing Initiative (Global) the CICC operates at the policy level to set priorities, direct research, and prepare advisory recommendations to the Attorney General. It consists of representatives from law enforcement and homeland security agencies who advocate for criminal intelligence sharing among SLTT law enforcement to promote public safety and homeland security. PM-ISE collaborates with the CICC to coordinate national-level information sharing initiatives in a number of their focus areas.

Partners: DOJ, DHS.

Association of State Criminal Investigative Agencies (ASCIA) Engagement

PM-ISE participates in events and provides subject matter expertise to the overall organization specifically on human trafficking, state & regional ISE development, officer involved shootings/use of force, and police data collection. Expect to continue active participation in FY17 and beyond.

Partners: ASCIA Membership.

Request for Information (RFI) Implementation

Create a common process across all levels of government for RFIs to enable timely receipt and dissemination of information and appropriate response.

Partners: Information Sharing and Access Interagency Policy Committee (ISA-IPC) RFI Working Group

Alerts Warning and Notifications (AWN) Implementation

Create a common process across all levels of government for AWN to enable timely receipt and dissemination of information and appropriate response.

Partners: ISA-IPC AWN Working Group

Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI)) Implementation

Complete the implementation of NSI programs with the National Network of Fusion Centers and Federal entities while expanding training and outreach beyond law enforcement to the rest of the public safety community.

Partners: Responsible Information Sharing (RIS) Subcommittee (SC), NSI Program Management Office (PMO)

Counterterrorism (CT)

Portfolio work addresses information sharing deficiencies associated with the CT mission both directly and tangentially. Previously focused almost exclusively on Watchlisting, Screening, and Encounters of persons or activity related to terrorism. The recent rise of homegrown terrorism has brought opportunities to leverage information sharing and a national perspective to local partners' Countering Violent Extremism (CVE) efforts.

Goal: Streamline agency-to-agency policies, procedures, and capabilities to improve the sharing of terrorism-related information, enabling the identification of foreign and homegrown violent extremists and the prevention of terrorist acts.

Domain Awareness

Several key domains have been identified where terrorist exploitation or corruption could pose devastating nationwide impacts. Currently the portfolio is focused on Critical Infrastructure Key Resources (CIKR), Maritime, and Air Domains.

Goal: Identify, innovate & deploy repeatable processes & tools that will cultivate responsible information sharing, partnerships among Federal, State, Local, Territorial, Tribal, Private Sector (FSLTTPS) to improve the security, safety, and economic resilience of our critical infrastructure and transportation domains.

Private Sector Information Sharing Implementation

Establish ISE-related information sharing processes and sector-specific protocols with private sector partners to improve information quality and timeliness as well as secure the nation's infrastructure.

Partners: DHS, FBI, Cyber Interagency Policy Committee (IPC), NSC.

Private Sector Information Sharing

Establish ISE-related information sharing processes and sector-specific protocols with private sector partners to improve information quality and timeliness as well as secure the nation’s infrastructure.

Partners: DHS, FBI, Cyber Interagency Policy Committee (IPC), NSC.

Cybersecurity Information Sharing

The extent to which we rely on information exchanged in cyberspace directly impacts our exposure to terrorist exploitation of inherent vulnerabilities. PM-ISE is uniquely positioned, due to our longstanding relationships with FSLTTPS entities, to foster responsible information sharing practices that safeguard national security, enhance law enforcement investigations, and provide needed context of intelligence analysts to protect and defend these exchanges.

Goal: Connect and integrate federal and non-federal partners with each other and with solutions to enhance cyber information sharing.

Cyber Analyst Exchange Pilot

Facilitates placement of US Cyber Command (USCYBERCOM) trainees at Fusion Centers so Centers get a highly skilled and motivated analyst for a fraction of the market price (lodging and per diem) while simultaneously relieving USCYBERCOM from pressure created by their external tour requirement.

Partners: Fusion Centers, DOD, USCYBERCOM.

Tailored Cyber Threat Intelligence Integration Center (CTIIC) Products for State & Local Customers

Identify cyber intelligence requirements currently not being met by federal cyber intelligence organizations. In close coordination with those federal organizations, launch a pilot project where Office of the Director of National Intelligence (ODNI) CTIIC would tailor analytic products at the UNCLASSIFIED or SECRET level to meet those needs, routing the products though the appropriate channels for dissemination.

Partners: ODNI CTIIC, FBI, DHS.

Cybersecurity Stakeholder Engagement

ASCIA identified cybercrime as a top priority and created a cybercrime workgroup to address their member’s needs. Recent work included a PM-ISE funded ASCIA Cybercrime Workshop, the findings and next steps of which were provided to the 1 May 2016, ASCIA Cybercrime Subcommittee and coordinator of the NVPS Coordinating Meeting.

Partners: ASCIA, IACP, NFCA, FBI, DHS, IIR, BJA.

Association of State Criminal Investigative Agencies (ASCIA) Cybercrime Work Group Engagement

ASCIA identified cybercrime as a top priority and created a cybercrime workgroup to address their member's needs.

Partners: ASCIA, IACP, NFCA, FBI, DHS, IIR, BJA.

Sensitive But Unclassified (SBU) Information Sharing

Overcoming the barriers that impede controlled unclassified information sharing (CUI) is a continuing endeavor of the SBU information sharing portfolio. This sharing is critical because key contributors to law enforcement, public safety, and homeland security often cannot access the information they need because it is stored in disconnected, compartmentalized, restricted, or even classified networks.

Goal: Advance SBU information sharing services across a broad set of stakeholders to responsibly share timely, accurate, and compressive law enforcement, public safety, and homeland security information.

Identity, Credential, and Access Management (ICAM)

A significant hurdle to information sharing is establishing trust and interoperability among organizations that want to share information. Expressions of intent and the use of open system technologies alone are not enough. PM-ISE has developed a Federated ICAM (FICAM) portfolio that leverages an assertion based architecture implementation, (primarily Trustmarks – digitally signed assertions by a third party shared between two or more parties) to enable interoperability between partners.
Goal: Advance federated ICAM across prioritized Communities of Interest and identify opportunities for expansion to other communities.

Componentization of Criminal Justice Information Services (CJIS) Security Policy (using Trustmarks)

Development and deployment to a government accredited hosting environment using the Attribute Metadata Service and Federal Registry for US Federal Agencies with an initial operating capability to support three agencies and the ability to expand rapidly to others.

Partners: DoD, Office of Personnel Management (OPM), GSA, CJIS, GTRI, National Strategy for Trusted Identities in Cyberspace (NSTIC).

Origin Network Identity Exchange (ONIX)

Accelerate the CIO Council Project for the ONIX Initial Operating Capability (IOC) with DOD, GSA, and OPM. Design should support the use case for vetting visiting employees and detailed/transferring employees (among others) and address long term operational deployment beyond the initial three participants. GSA will provide ongoing operations and maintenance of the metadata service as a shared resource/service of common concern for partners on the

SBU/CUI fabric.

Partners: GSA, OPM, DOD.

Componentization of Privacy Policies Project (Trustmarks)

Develop a set of harmonized Trustmark Definitions (TD) based on those already developed in previous projects (GTRI’s NSTIC Trustmark pilot and the PM-ISE Componentization of CJIS Security, SP 800-53 and Personal Identity Verification Interoperability (PIV-I) Policy (using Trustmarks)) with over fifteen privacy source documents.

Partners: GTRI, DOD.

National Identity Exchange Federation (NIEF) DoJ Trustmark Pilot for Federated ICAM

A pilot for DOJ to implement a comprehensive strategy for engaging in federated ICAM with its SLT partners, as well as other US federal agencies leveraging the Trustmark Framework and the NIEF. The strategy will enable secure, trusted, bidirectional information sharing based on Attribute-Based Access Control (ABAC) between the DOJ and its partner agencies. Initially a DOJ Office of the Chief Information Officer (OCIO) pilot, the long-term vision is DOJ-wide adoption. Provides a real-world proof of concept of the ICIF Assertion Based Architecture.

Partners: DOJ, NEIF.

Assertion Authoring and Publishing Capability

A cloud based capability that allows external partners to develop and publish TDs and Trustmark Interoperability Profiles (TIP). The capability will be initially available to support a core workspace, library workspace, ICIF workspace, Identity Ecosystem Steering Group (IDESG) workspace, Geospatial workspace, and GSA workspace.

Partners: IDESG, GRTI, SCC, GSA, DOD.

ICAM Requirements between FirstNet and NextGen 911

Participation and advising to support the FirstNEt/NextGen911 ICAM Working Group. Recent work includes reviews of the FICAM Services Framework and IDESG Functional model comparison, providing of use cases, and some discussions of future collaborations.

Partners: FCC, FirstNet.

ICAM Roadmap

Support partners in the development and approval of a new ICAM strategy. In June 2016 participated in the Intelligence Community (IC) Identity and Access Management (IdAM) SC and Service Provider Board which reviewed a proposed IdAM standards framework including potential standards for the IC CIO.

Partners: OMB, NSCS, GSA, IC CIO.

Privacy, Civil Rights, Civil Liberties (P/CRCL)

Privacy Support

IIR provides deep, unbiased expertise on P/CRCL issues including for various information sharing projects across the nation. Some of the distinct lines of effort, continued over multiple fiscal years, are tracked as separate enduring activities, specifically: Agency ISE P/CRCL Policies, Support P/CRCL Mission Processes, and Privacy Support to NSISS PO7 (Core Awareness Training (CAT)).

Partners: DOJ, BJA, IIR

Agency ISE P/CRCL Policies

An ongoing effort supported by internal PM-ISE personnel and IIR to implement ISE Privacy Guidelines at the nonfederal entity level (including the private sector).

Partners: IIR.

Support P/CRCL Mission Processes

An ongoing effort supported by internal PM-ISE personnel and IIR to support the mission processes of the PM-ISE in addressing ISE P/CRCL functions and activities including for strategic ISE planning initiatives, content development for the annual report, policy advice, outreach efforts, support to ISE mission partners, and content review.

Partners: IIR.

APPENDIX B – DHS Information Sharing Resources

Solution	Description
Trusted Internet Connection (TIC)[8]	Works to enable organizations to identify and consolidate Internet connections (http://www.dhs.gov/trusted-internet-connections). As content and applications move to public cloud providers, CS&C is collaborating with the Federal Risk and Authorization Management Program (FedRAMP) to apply a TIC approach (https://www.fedramp.gov/draft-fedramp-tic-overlay/)
Network Flow Collection	Provides the enterprise with an awareness of the type and volume of traffic flowing into (and out of) the enterprise network. Information includes source/destination IP address, domains, and ports. This data can be filtered and searched to identify anomalous flow patterns, and initiate further research into potential risks and attacks. Flow collectors are deployed at TIC locations, supporting Federal and State stakeholders. (https://msisac.cisecurity.org/about/services/)
Intrusion Detection (IDS)	DHS provides IDS sensors at TIC locations, and also develops digital signatures which are loaded into the IDS to identify threats. Organizations receiving this service are able to view alerts created by the IDS (occurring when signatures identify pattern matches in network traffic). This service is currently available to Federal and State stakeholders. (http://www.dhs.gov/cybersecurity-and-privacy)
Intrusion Prevention (IPS)	DHS deploys IPS to public and private network owners. IPS is similar to IDS in that digital signatures are used at the sensor. With IPS, when signatures identify pattern matches, countermeasure actions are taken such as dropping or rerouting traffic. While network flow collection and IDS are passive (i.e., monitoring and alerting) cybersecurity measures, IPS is an active security measure. (http://www.dhs.gov/cybersecurity-and-privacy)
Continuous Diagnostics and Mitigation (CDM)	DHS deploys CDM services, which include hardware and software asset management, configuration management, vulnerability management capabilities. These services are enabled through devices (physical and virtual) deployed inside the enterprise network, and presented to security professionals in a dashboard. For stakeholder organizations (currently only Federal Civilian Agencies), CDM is the major technology solution that supports the tenets of ongoing authorization. (http://www.gsa.gov/portal/content/177895)
Risk Assessment and Risk Analysis	DHS provides infrastructure baseline assessments, vulnerability assessments, impact assessments, and comprehensive risk and mitigation analyses of public safety infrastructure and services in conjunction with other departments and agencies, as well as individual PSAPs.

Figure 6 - DHS Office of Emergency Communications Offerings

Federal, State and Local Partnerships and Forums. DHS has formed existing relationships across all levels of government to inform the design and deployment of

Emergency Communication1 networks. DHS supports SAFECOM and the National Council of Statewide Interoperable Coordinators bringing State, local, Tribal, and Territorial perspective to a National forum. DHS has partnered with the U.S. Department of Transportation (DOT) NG9-1-1 Program Office to facilitate education and awareness of cyber security with the State and local community through the delivery of tools and training. DHS also facilitates the Emergency Communications Preparedness Center (ECPC) 9-1-1 Focus Group, which is dedicated to enhancing the resiliency of Federal PSAP operations.[9] Additionally, DHS manages the Emergency Services Sector (ESS) Cyber Working Group to evaluate cyber risks that the sector might encounter.

Assessments and Analysis. DHS, in conjunction with the DOT National 9-1-1 program, is currently developing an NG9-1-1 security best practice and self-assessment tool for PSAPs, Cyber Risks to Next Generation 9-1-1.[10] Additionally, DHS is working on next steps on the development of Identity, Credential, and Access Management (ICAM) for public safety and FirstNet's National Public Safety Broadband Network. The through the ESS Cyber Working Group mentioned above, the Department has published the DHS Internet Protocol (IP) Emergency Services Sector Cyber Risk Assessment[11] and Emergency Services Sector Roadmap to Secure Voice and Data Systems,[12] which provide pertinent guidance for public safety agencies, including those considering the adoption of NG9-1-1 technology and systems to strengthen their systems and networks against cyber risk through mitigation measures.

Public / Private Collaboration. The Critical Infrastructure Cyber Information Sharing and Collaboration Program (CISCP) establishes trusted cyber information sharing relationships across Government and Industry. CISCP facilitates the secure exchange of cybersecurity indicators, enabling organizations to protect themselves against emerging attacks. Currently, CISCP has over one-hundred member organizations and is working in collaboration with the NCCIC to automate cybersecurity information sharing amongst its members.[13]

User Training and Education. DHS provides resources for cybersecurity training and awareness, for use by any public or private entity. These resources can be leveraged to provide users with a basic level of awareness of cybersecurity risks. In many instances, cyber threat actors exploit untrained individuals (*e.g.*, phishing attacks) to gain initial access to the enterprise and initiate further actions. The "Stop. Think .Connect. Campaign" is geared to provide awareness.[14] DHS also supports the National Initiative for Cybersecurity Education (NICE), which provides additional educational resources for public and private organizations.[15] DHS also delivers education and technical assistance to Federal, State and local public safety community on PSAP deployments.

Outreach and Assistance. The Critical Infrastructure Cyber Community C³ (pronounced "C Cubed") Voluntary Program (C^3VP) supports organizations of all sizes to establish or

[9] Office of Emergency Communications, http://www.dhs.gov/office-emergency-communications.
[10] Cyber Risks to Next Generation 9-1-1, available at http://www.dhs.gov/office-emergency-communications .
[11] DHS Internet Protocol (IP) Emergency Services Sector Cyber Risk Assessment. https://www.dhs.gov/sites/default/files/publications/Emergency-Services-Sector-Cyber-Risk-Assessment-508.pdf
[12] ESS Roadmap to Secure Voice and Data Systems. https://www.dhs.gov/sites/default/files/publications/Emergency-Services-Sector-Roadmap-to-Secure-Voice-and-Data%20Systems-508.pdf
[13] (https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity)
[14] (http://www.dhs.gov/stopthinkconnect)
[15] (http://csrc.nist.gov/nice/index.htm)

improve their cyber risk management processes and to take advantage of free technical assistance, tools, and other resources offered by the U.S. Government. C^3VP can assist PSAPs in understanding how to use NIST's Cybersecurity Framework and other risk management efforts.

DHS National Cybersecurity & Communications Integration Center (NCCIC)

Information sharing is a key part of the Department of Homeland Security's (DHS) mission to create shared situational awareness of malicious cyber activity. Cyberspace has united once distinct information structures, including our business and government operations, our emergency preparedness communications, and our critical digital and process control systems and infrastructures. Protection of these systems is essential to the resilience and reliability of the nation's critical infrastructure and key resources; therefore, to our economic and national security. DHS's National Cybersecurity and Communications Integration Center (NCCIC) is a 24x7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the Federal Government, intelligence community, and law enforcement.

The NCCIC shares information among public and private sector partners to build awareness of vulnerabilities, incidents, and mitigations. Cyber and industrial control systems users can subscribe to information products, feeds, and services at no cost.

NCCIC Vision

The NCCIC vision is a secure and resilient cyber and communications infrastructure that supports homeland security, a vibrant economy, and the health and safety of the American people. In striving to achieve this vision, the NCCIC will:

- Focus on proactively coordinating the prevention and mitigation of those cyber and telecommunications threats that pose the greatest risk to the nation.
- Pursue whole-of-nation operational integration by broadening and deepening engagement with its partners through information sharing to manage threats, vulnerabilities, and incidents.
- Break down the technological and institutional barriers that impede collaborative information exchange, situational awareness, and understanding of threats and their impact.
- Maintain a sustained readiness to respond immediately and effectively to all cyber and telecommunications incidents of national security.
- Serve stakeholders as a national center of excellence and expertise for cyber and telecommunications security issues.
- Protect the privacy and constitutional rights of the American people in the conduct of its mission.

The NCCIC includes the following branches:

- United States Computer Emergency Readiness Team (US-CERT);
- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT); and
- National Coordinating Center for Communications (NCC).

As mutually supporting, fully integrated elements of the NCCIC, these branches provide the authorities, capabilities, and partnerships necessary to lead a whole-of-nation approach to addressing cybersecurity and communications issues at the operational level.[16]

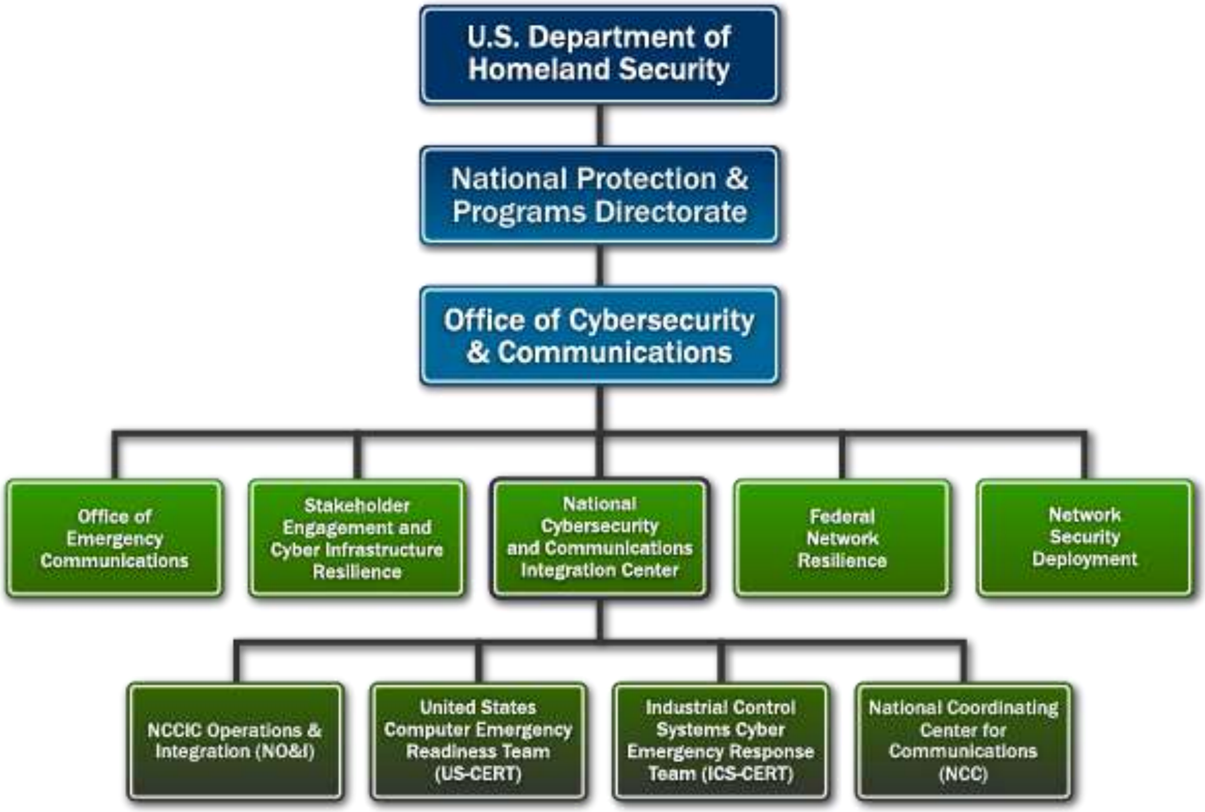

U.S. Department of Homeland Security
National Protection & Programs Directorate
Office of Cybersecurity & Communications
Office of Emergency Communications
Stakeholder Engagement and Cyber Infrastructure Resilience
National Cybersecurity and Communications Integration Center
Federal Network Resilience
Network Security Deployment
NCCIC Operations & Integration (NO&I)
United States Computer Emergency Readiness Team (US-CERT)
Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
National Coordinating Center for Communications (NCC)

Figure 7 - NCCIC Org Chart (Source – US Dept. of Homeland Security)

US-CERT

United States Computer Emergency Readiness Team (US-CERT) brings advanced network and digital media analysis expertise to bear on malicious activity targeting our nation’s networks. US-CERT develops timely and actionable information for distribution to federal departments and agencies, state and local governments, private sector organizations, and international partners. In addition, US-CERT operates the National Cybersecurity Protection System (NCPS), which provides intrusion detection and prevention capabilities to covered federal departments and agencies.

US-CERT strives for a safer, stronger Internet for all Americans by responding to major incidents, analyzing threats, and exchanging critical cybersecurity information with trusted partners around the world.

US-CERT’s critical mission activities include:

- Providing cybersecurity protection to Federal civilian executive branch agencies through intrusion detection and prevention capabilities.

[16] https://www.dhs.gov/national-cybersecurity-and-communications-integration-center

- Developing timely and actionable information for distribution to federal departments and agencies; state, local, tribal and territorial (SLTT) governments; critical infrastructure owners and operators; private industry; and international organizations.

- Responding to incidents and analyzing data about emerging cyber threats.

- Collaborating with foreign governments and international entities to enhance the nation's cybersecurity posture.

ICS-CERT

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among Federal, state, local, and tribal governments and control systems owners, operators, and vendors. Cybersecurity and infrastructure protection experts from ICS-CERT provide assistance to owners and operators of critical systems by responding to incidents and helping restore services, and by analyzing potentially broader cyber or physical impacts to critical infrastructure. Additionally, ICS-CERT collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures.

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among Federal, state, local, and tribal governments and control systems owners, operators, and vendors. Additionally, ICS-CERT collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures.

NCC

In January 2000, the White House designated NCC as the Information Sharing and Analysis Center (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 government and industry telecommunications participants.

As part of the Department of Homeland Security's (DHS) National Cybersecurity and Communications Integration Center (NCCIC), the National Coordinating Center for Communications (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.

The NCC leads and coordinates the initiation, restoration, and reconstitution of National Security and Emergency Preparedness telecommunications services or facilities under all conditions. NCC leverages partnerships with government, industry and international partners to obtain situational awareness and determine priorities for protection and response.

With much of the nation's cyber infrastructure tied into communications, the NCC

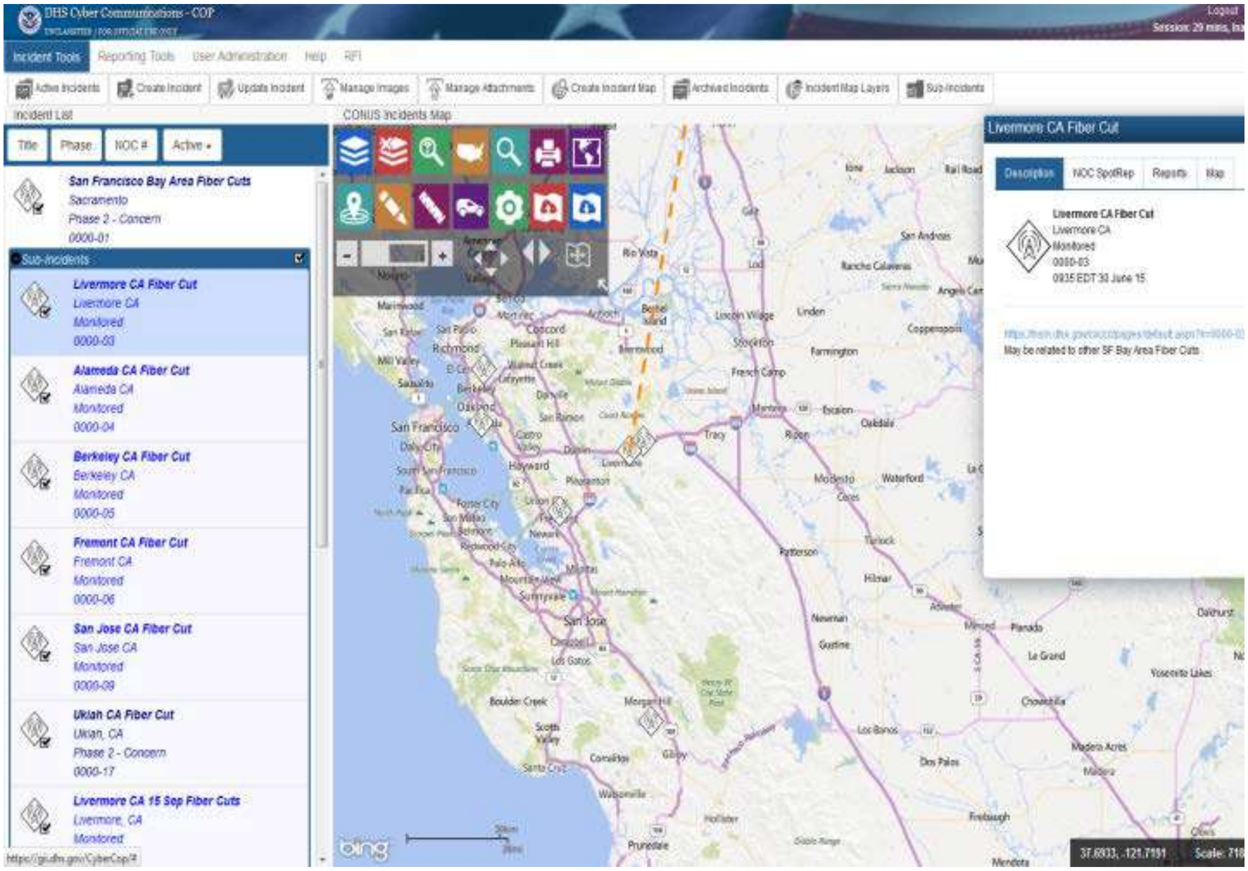
Watch is also a vital partner to the national cybersecurity effort. The NCC works with both the U.S. Computer Emergency Response Team (US-CERT) and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) to monitor and resolve issues impacting cyber and communications during an emergency.

NCC Watch cannot perform its vital mission without the cooperation and expertise of its federal and private sector partners. It was the private sector that first recommended the establishment of a centralized government-industry coordination center following the divestiture of AT&T in the early 1980s. Today, 24 federal government agencies and over 50 private sector communications and information technology companies routinely share critical communications information and advice in a trusted environment to support the NCC's national security/emergency preparedness communications mission.[17]

DHS Common Operating Picture (COP)

The DHS Common Operating Picture provides government and private sector decision makers with enhanced situational awareness, facilitating timely decision support prior to or in the aftermath of a natural disaster, act of terrorism, or other man-made disaster. The DHS COP architecture coupled with data from Homeland Security partners provides actionable information, enhanced contextual understanding, and geospatial awareness. This enables government and private sector leaders to make timely and informed decisions, and identify courses of action during an event or threat situation. The DHS COP provides users a broad set of capabilities based on best-in-class technologies that deliver a rich end user experience through a web-accessible interface. These core capabilities include role-based access, merging and displaying incident-specific information in multiple formats, data ingest and triage, alerts and notifications, and map visualization.

[17] https://www.dhs.gov/national-coordinating-center-communications



San Francisco Bay Area Fiber Cuts
Sacramento
Phase 2 - Concern
0000-01

Livermore CA Fiber Cut
Livermore CA
Monitored
0000-03

Alameda CA Fiber Cut
Alameda CA
Monitored
0000-04

Berkeley CA Fiber Cut
Berkeley CA
Monitored
0000-05

Fremont CA Fiber Cut
Fremont CA
Monitored
0000-06

San Jose CA Fiber Cut
San Jose CA
Monitored
0000-09

Ukiah CA Fiber Cut
Ukiah, CA
Phase 2 - Concern
0000-17

Livermore CA 15 Sep Fiber Cuts
Livermore, CA
Monitored

Livermore CA Fiber Cut

Livermore CA Fiber Cut
Livermore CA
Monitored
0000-03
0935 EDT 30 June 15

https://hsin.dhs.gov/cc/pages/default.aspx?i=0000-03
May be related to other SF Bay Area Fiber Cuts

Figure 8 - DHS Common Operating Picture

CC-COP

In support of Executive Order 13618, the Department of Homeland Security (DHS) Cyber Communications Common Operating Picture (CC-COP) provides federal-state-local-tribal and territorial government and critical infrastructure owners and operators coordinated situational awareness enabling state and federal leadership to prioritize response to crisis cyber or communications incidents impacting Business Essential Functions or Mission Essential Functions, which protect our communities and nation: Facilitating timely decision support prior to or in the aftermath of a natural disaster, acts of terrorism, or man-made disaster. The CC-COP architecture coupled with data from DHS partners and Homeland Security Information Network (HSIN) provides actionable information, enhanced contextual understanding, and geospatial awareness. The following high-level capabilities of the CC-COP provide information sharing capabilities that may be of use to public safety communications.

- User Interface:
  Allows users to access all COP capabilities via a customizable dashboard.

- Role-Based Access:
  Provide a customized COP experience based on a specific role.

- Incident Management:
  Create, visualize and display incident information in a common operating picture available to all HLS partners

- Map Visualization:
  View geo-extracted, auto-ingested information and create user-defined views of incident information.

- Reporting:
  Create, edit and update multiple reports for the Homeland Security community.

- Alerts/ Notifications:
  Automatically alert users when information of interest is received or incidents are

State and Major Urban Area Fusion Centers

In coordination with the NOC/IW, state and major urban area fusion centers share threat-related information between the federal government and state, local, tribal, territorial, and private sector partners. Located in states and major urban areas throughout the country, fusion centers conduct analysis and facilitate information sharing while assisting law enforcement and homeland security partners in preventing, protecting against, and responding to crime and terrorism. Fusion centers are owned and operated by state and local entities with support from federal partners in the form of deployed personnel, training, technical assistance, and exercise support.