EXECUTIVE SUMMARY
Joint Meeting of SAFECOM and the
National Council of Statewide Interoperability Coordinators (NCSWIC)
May 13, 2015, Crowne Plaza, Jacksonville, Florida

A MESSAGE FROM THE DEPARTMENT OF HOMELAND SECURITY (DHS) OFFICE OF EMERGENCY COMMUNICATIONS (OEC) DEPUTY DIRECTOR CHRIS ESSID

Chris Essid, OEC Deputy Director, kicked off the joint session by emphasizing the integral role stakeholder groups like SAFECOM and NCSWIC play setting OEC priorities. Mr. Essid noted that OEC wants to return to its roots and focus mainly on stakeholder-driven input by integrating feedback from stakeholders into OEC-developed products and services. OEC's stakeholders are at the forefront of evolving emergency communications, and the needs and insights of the public safety community continue to shape the future of OEC priorities. Mr. Essid asked members for feedback on the services and guidance OEC can offer stakeholders to encourage current priorities, such as statewide governance. Mr. Essid encouraged participants to consider how OEC can further support stakeholder priorities and initiatives throughout the meeting.

CROSS BORDER COLLABORATION FOR INTEROPERABILITY: THE NOTHERN BORDER

Rick Andreano, OEC New England Coordinator, moderated a panel on northern border interoperability collaboration between the United States (U.S.) and Canada. Panelists included Barry Luke, National Public Safety Telecommunications Council (NPSTC); Jim Jarvis, Region OEC Great Lakes Region Coordinator; Dan Hawkins, Region OEC Rocky Mountain Region Coordinator; and Robert Barbato, New York Statewide Interoperability Coordinator (SWIC).

Mr. Luke began the discussion by explaining how NPSTC has been coordinating with their Canadian counterparts, the Canadian Interoperability Technology Interest Group (CITIG), on issues related to the regulatory environment surrounding cross-border communications interoperability. He also shared information about the joint Cross Border Communications Report, a collaborative effort among organizations, including 31 recommendations organized into the five lanes of the Interoperability Continuum (Governance, Standard Operating Procedures, Technology, Training and Exercises, and Usage). Cross border public safety communications is often challenging due to a variety of communications and procedural issues that involve regulatory processes, technology, and governance matters. The inability to directly communicate with other emergency responders puts property, the lives of responders, and the public they seek to protect at risk. Fire departments and Emergency Medical Service (EMS) units from both countries routinely respond across the border for first response and mutual aid support. State and local law enforcement units rarely cross the border, but federal law enforcement teams, such as Integrated Border Enforcement Teams (IBET) and U.S./Canadian joint task forces, work along the border.

Mr. Luke discussed priorities that were identified for further study during a 2010 cross border meeting between OEC and Public Safety Canada, in which three scenarios (Figure 1) were identified for immediate action:

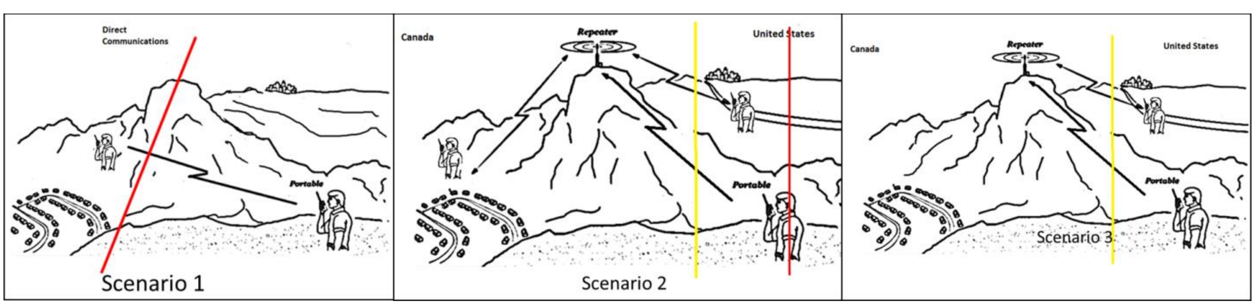


Figure 1: Cross Border Communication Scenarios

- *Scenario 1:* Operation of mobile and/or portable radio transceivers on the other side of the border in the "direct" (non-repeater) mode
- *Scenario 2:* Use of base station repeaters on the other side of the border to interoperate with public safety officials in the other country

- *Scenario 3:* Use of base station repeaters on the other side of the border to communicate with public safety officials in their own country

The Federal Communications Commission (FCC) and Industry Canada have made great strides to improve interoperable communications through treaty updates clarifying the use of portable radios at and across the border (i.e., Scenario 1). Both are working to develop solutions to the two remaining scenarios described above. The FCC and Industry Canada are also coordinating on the public safety licensing process. The *Pacific Northwest Emergency Management Compact*, which covers Alaska, Idaho, Oregon, Washington, British Columbia, and the Yukon Territory, provides automatic cross border credentialing and licensing for Emergency Medical Technicians, paramedics, and firefighters. There are also numerous best practices and local agreements in place to help facilitate interoperable communications.

Mr. Andreano noted that there are existing interoperability issues between jurisdictions within the U.S. that are compounded by border issues. Mr. Andreano and Chris Tuttle (OEC Region II Coordinator) are working with the northeast US states of Maine, New Hampshire, Vermont, and New York to make communications within the U.S. more interoperable through the common licensing of the VCALL10 as a hailing channel and coordination of National Interoperability Channels and State mutual aid channels.

Mr. Barbato discussed interoperable communications challenges along the New York border. He noted that the biggest problem lies in frequency coordination and licensure, which is beyond the control of stakeholders in the region. Instead, the state has focused on the tactical side of response coordination. Planned events provide an excellent venue for working relationships between the countries. New York has been focused on problem solving and coordination between U.S. and Canadian authorities as well as with neighboring U.S. jurisdictions in and around New York. He noted that the base station approach is a very practical solution that avoids the larger frequency issues. Federal agencies operating along the border have similar concerns and are often trying to solve the same problems. New York has considered working with state and federal counterparts to develop common channels and resources along both sides of the border in the future. Mr. Andreano agreed that there is more power behind the public safety community when there are multiple states and provinces cooperating to solve the issues.

Mr. Jarvis noted that Ontario is upgrading their systems and is leveraging U.S. subject matter experts, such as SWICs Brad Stoddard (Michigan) and Darryl Anderson (Ohio). Mr. Jarvis described how he became aware of the border communications issues through his work with DHS Customs and Border Protection in 2003, when he worked with IBET teams to identify communications best practices and lessons learned along the border. Gateway-type devices were installed with U.S. and Canadian receivers across the border, in coordination with the National Telecommunications and Information Administration (NTIA). Smaller pilot projects evolved into Internet Protocol (IP)-based solutions. The region faced obstacles including encryption requirements (some of which were solved through IP gateways), radio frequency broadcasts, and dispatch operators encountering differing privacy laws between the two countries. He emphasized that it was more helpful to think of the situation in terms of “thinking globally and acting locally.” As another potential solution, Mr. Andreano noted that Maine was awarded the Border Interoperability Demonstration Project (BIDP) grant, in which one initiative was the purchase of cache radios that could be issued to local responders when crossing the border.

Mr. Hawkins explained that he is the OEC Coordinator for the Rocky Mountain Region, comprising approximately 800 miles of the Canadian-U.S. border filled with national and international parks. He noted that, in the past, terrorists have used this region to cross the border as it is so sparsely populated. The biggest natural disaster in the area is caused by the annual Red River flooding. There are also large tribal nations in the region with their own communications needs. Mr. Hawkins also described the long history of frequency coordination issues, most of which result from “Line A” issues that require additional Canadian frequency coordination if the area is within a designated distance from the Canadian-U.S. border. While mountains make good locations for radio towers, as a signal can reach for 100 miles in any direction, finding a frequency that does not interfere with Canadian frequencies remains a challenge. Montana re-energized use of the VLAW31 channel along and across the border as a solution. Both the U.S. and Canada used the frequency with no issues for many years under FCC designation as a national law enforcement interoperability frequency, as it is largely open with no interference issues. As part of the Montana BIDP assistance, the state licensed additional frequencies and filed a waiver with the FCC to expand use of VLAW31 to fire, EMS, and law enforcement. Mr. Luke noted that following issuance of the FCC waiver for VLAW31, Montana opened its online permitting system to Canadian agencies. The system is used to permit other agencies and organizations access to shared frequencies licensed by the state. Montana made additional modifications to allow Canadians to access the site. Industry Canada now also allows the use of the channel in Canada. Montana also participated in the Western vignette for the Canada-U.S. Enhanced Resiliency Experiment (CAUSE) III in 2014 to test cross border action capabilities and deployable long-term evolution systems. Mr. Andreano noted that portions of CAUSE III focused on social media were conducted in the New England region as well.

Dan Wills (SAFECOM, Arizona State Forestry) asked if states are also leveraging NTIA spectrum. Mr. Luke noted that the recent agreement between Industry Canada and the FCC did not include NTIA. Mr. Jarvis added that the FCC/Industry Canada Letters of Intent (for the three scenarios) have not included NTIA spectrum. Mr. Hawkins noted it has been used for the Montana trunked system, including BIDP-funded sites, and suggested keeping the NTIA option included for cross-border communications.

Darryl Ackley (SAFECOM, National Association of State Chief Information Officers) noted that New Mexico is exploring the use of spectrum along the U.S.-Mexico border and is facing governance and funding/sustainability issues. Mr. Luke noted that there has not been significant discussion about sustainability, but there are concerns about how to install capabilities that meet the community's needs and provide long-term, sustainable funding. Along the southern border, DHS has worked to leverage federal solutions to assist at the local level through the use of IP-gateways for U.S. cities to obtain access to Mexican tower sites.

Tom Roche (SAFECOM, New York State Office of Public Safety) noted that counties in New York, located 70 miles from the border, have applied for radio licenses and public safety agencies that need frequencies still cannot get them, which results in overcrowding. He emphasized the need to balance the importance of localities right along the border with those further away, and that localities distant from the border do not seem to get the same attention as those right along the border, leading to agencies renouncing the request process. Mr. Andreano noted that with some socialization prior to applying for frequencies and greater understanding of the licensing process, agencies may be able to obtain the frequencies needed, but cautioned that it can be a labor-intensive process. Mr. Barbato agreed that it is more helpful to talk to an individual rather than an agency. Furthermore, Mr. Andreano suggested that being able to socialize funding/grants issues (i.e., deadlines) to representatives from both granting authorities (i.e. FEMA GPD) and regulatory agencies (i.e. FCC/NTIA/Industry Canada) can help expedite management of the issue.

Steve Proctor (SAFECOM Chair, Utah SWIC, Utah Communications Authority) asked if there was any Public Safety Answering Point (PSAP) interaction across the border. Mr. Jarvis noted several instances of PSAP to PSAP interaction, such as through the Virtual USA initiative in Michigan, which is designed to improve decision making for local, state, tribal, and federal homeland security practitioners through the collection and consolidation of interagency situational awareness data.

OFFICE FOR INTEROPERABILITY AND COMPATIBILITY

Dan Cotter, Acting Director of S&T Directorate's First Responders Group (FRG), provided an overview of current initiatives within OIC. The FRG oversees research for the development of tools and technologies that help the Next Generation First Responder (NGFR), particularly under its Apex Program. Apex takes a deeper look at border situational awareness, real-time bio threat analysis, airport screening and security, and flood awareness. The NGFR program focuses on improving uniforms with smart technology, personal devices, and video to help analyze emergency situations before responders arrive on the scene. With the Communications and Network Engine and Situational Awareness/Decision Support, geographic information systems (GIS) play an important role in the development and implementation of these technologies. Additionally, OIC launched a prize competition to challenge those interested to find solutions for indoor tracking.

Attendees sought Mr. Cotter's thoughts on the data collected by body-worn cameras and other new technology that may affect evidence collected by first responders. Mr. Cotter confirmed that it is typically up to the individual organization using the equipment to monitor and control data and appoint access to information. John Contestabile (Johns Hopkins University) noted that the Public Safety Communications Research program's Video Quality in Public Safety Working Group will meet in June to discuss video and data retentions and provide recommendations on policies for growing technology needs.

OIC continues to provide science and technology that enables emergency communications and facilitates the seamless exchange of information to save lives and protect property. Mr. Cotter looks forward to building and maintaining a lasting relationship with SAFECOM and NCSWIC to glean the subject matter expertise that its members have to offer.

CYBERSECURITY THREAT MITIGATION

NCSWIC and SAFECOM members heard from a panel of experts on issues related to cyber security, including the Cyber Security Continuum and the National Institute of Standards and Technology (NIST) Cybersecurity Framework. Panelists included Chris Lombard, SAFECOM, Interagency Board (IAB); Traci Knight, DHS, OEC; Mark Hogan, City of Tulsa Asset Management Department, Director; and George Perera, SAFECOM, Miami-Dade Police Department. Although not in attendance, Jim Cronkhite, NORAD-USNORTHCOM, Cyber Current Operations Division, Deputy Chief, provided significant presentation content for the discussion, which was covered by the other panelists.

Mr. Lombard began the discussion by noting state Chief Information Officers' (CIO) continuous challenge identifying and implementing proactive and preventative cybersecurity programs in response to the emergency services sector's ever-increasing need to protect and manage data. In response, the Interagency Board developed the Cybersecurity Continuum, a supporting tool to assist leaders and managers in both assessing their current cyber readiness posture and assisting in making critical cyber security decisions[1]. A snapshot of the Cybersecurity Continuum was provided to SAFECOM this past year, detailing the public safety community's current position and achievements in cybersecurity, future goals, and steps for achieving these goals. The vision for the IAB Cybersecurity Continuum is to enable non-Information Technology (IT) or Information Systems (IS) leaders and managers to understand and quantify cybersecurity maturity levels and devote the appropriate resources to meeting cybersecurity challenges. In a similar vein, the National Institute of Standards and Technology (NIST) created the Cyber Security framework aimed at providing an in-depth structure used to create, guide, assess, or improve comprehensive cybersecurity programs[2]. As Mr. Lombard noted, the framework provides an incredible amount of detail, perhaps minimizing its utility. In an effort to improve both documents, the IAB and NIST partnered to examine overlapping features and opportunities to leverage information for improvement. Both organizations hope to blend the documents to create guidance appropriate for senior-level managers and officials.

Ms. Knight, OEC's Technology Policy Program Lead within the Policy and Planning Branch, provided high-level definitions of cybersecurity and associated terms, including cyber infrastructure, risk, and vulnerability. She noted how the term "cyber" is often used interchangeably to describe both cybersecurity and cyber infrastructure. Cyber risk, she clarified, is the likelihood a threat will exploit a vulnerability and the potential consequence or impact of that event. OEC realizes that emergency response communications is made up of more than just the networks (i.e., National Public Safety Broadband Network [NPSBN], commercial provider wireless networks); it also involves users' devices and equipment, their network connections, and data, applications, and

Cyber Definitions: Clarifying Terms

Cyber infrastructure is: "Electronic information and communication systems and information contained in these systems…Comprised of both hardware and software that process, store, and communicate data of all types"

Cybersecurity is: "The prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of [cyber infrastructure] to ensure confidentiality, integrity, and availability"

[1] https://iab.gov/Uploads/IAB%20Cyberspace%20Security%20Continuum.pdf
[2] http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm

services. OEC continues to work with stakeholders on issues related to database and Next Generation (NG 9-1-1) security. These systems, including both their hardware and software, are only as strong as their weakest link, and exposing vulnerabilities at an early stage is an important step toward mitigating threat. Ms. Knight provided additional background on the NIST Cybersecurity Framework, a major component of the Presidential Executive Order (EO) 13636, *Improving Critical Infrastructure Cyber Security*. The document itself is complex, making it easy for an IT manager or systems administrator to understand but difficult for the public safety community to interpret.

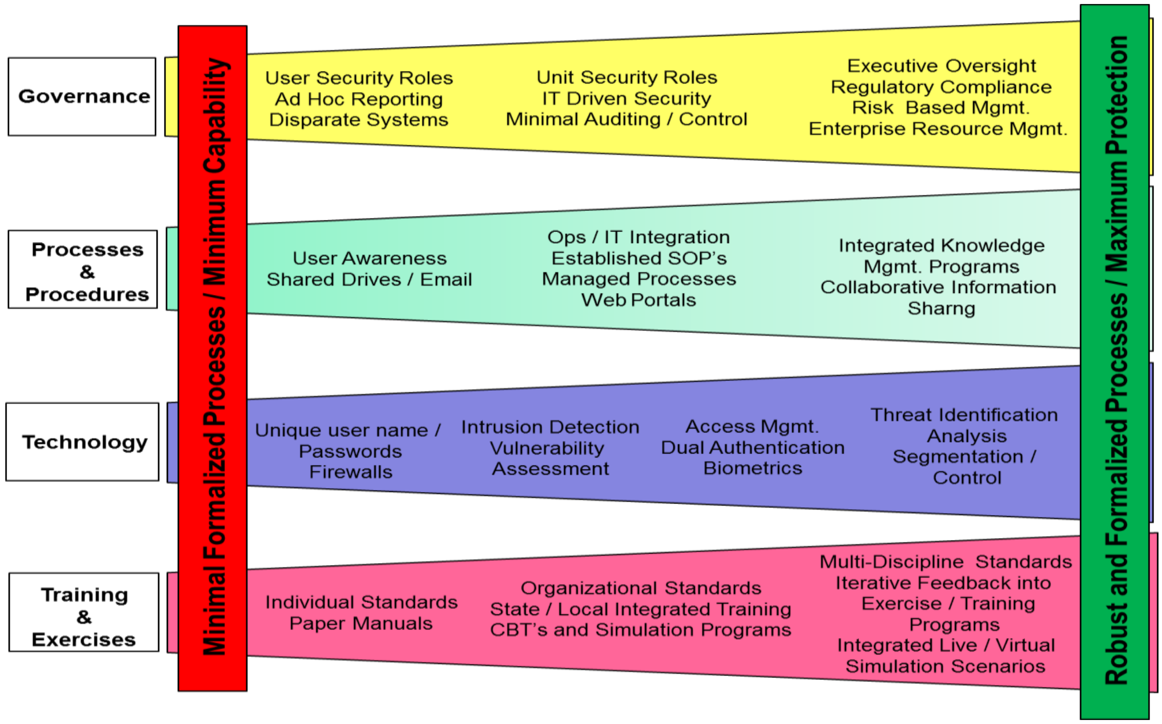


Figure 2. The Cybersecurity Continuum

Ms. Knight also provided information on federal programs aimed at reducing cyber risk and threat, including the Critical Infrastructure Cyber Community (C3) Voluntary Program and the Cyber and Physical Threat and Risk Analysis to Improve Networks (CAPTAIN) program. C3 encourages use of the Framework to strengthen critical infrastructure cybersecurity and acts as the central coordination point for the federal government for those interested in improving cyber risk management processes. Initial support resources will come from DHS, but will expand to include those as a result of partnerships with the private sector and industry, and across state and local governments. CAPTAIN's mission is to increase the understanding and awareness of emergency communications stakeholders about critical cyber and physical risks that could threaten the mission of first responders and public safety agencies.

Mr. Hogan, self-described as a jack of all trades, attributed his position as Tulsa CIO to his vast awareness of the cybersecurity challenges states and localities face. In this position, Mr. Hogan became aware of the need to apply all lanes of the continuum (i.e., governance, training and exercises, technology, usage, processes) to Tulsa's cybersecurity efforts (see Figure 2), and how to use those lanes to promote robust and formalized processes and maximize protection. Shifts in thinking about protection extend past physical security to include a new vulnerability: gaining access to or stealing virtual data.

Mr. Perrera, a specialist in cyber security concerns, used the continuum as a guideline to remind stakeholders that these efforts begin with physical security, but also require extensive methods for monitoring and identifying cyber threats, the development and implementation of a detailed response plan, and strategies for recovering data. Recovery also includes managing knowledge, further assessing vulnerabilities, analyzing how data may be exploited, and testing and evaluating systems. Mr. Perrera mentioned that OEC offers training on cybersecurity through their website. In a continuing conversation, Mr. Hogan emphasized the difficulty rationalizing the need to acquire critical infrastructure protection funding. He also urged stakeholders to "think outside the box" and consider long-term disruptions for states and localities, such as major attacks on public infrastructure resulting in the loss of public confidence. As former Washington CIO, Bill Schrier (Washington Deputy SWIC) experienced 1000's of attempts each day, and noted that in some cities, outside firms are hired specifically to conduct penetration testing of the their systems. Mr. Lombard emphasized the need for cities to create checklists to make it harder for hackers to gain access to systems. Suggestions for fortifying systems from other audience members included: look at how the corporate world protects against cyber threats; encourage conversations between IT specialists and operations personnel; continue to develop automated detection technologies; identify shortcomings in technology, funding, training and exercises and reporting up; and if possible, rely on the collective efforts of your team.

COMMITTEE WORKING SESSIONS

Technology Policy

Following the Cybersecurity Threat Mitigation panel, the cybersecurity breakout session, hosted by the joint Technology Policy Committee, provided a forum for members to share personal experiences and opinions on cybersecurity and to contribute to the Cybersecurity Primer work product. Participants were split into 8 groups and asked to work through a set of cybersecurity questions. Facilitators at each table moderated discussions around cyber challenges, the current emergency communications landscape, and cyber resources, such as the NIST Framework and the Cybersecurity Continuum.

Several key themes emerged during the session. For instance, many participants shared their organization's experiences with cyber attacks, which included denial of service attacks, malware, and email and phishing schemes, as well as threats introduced through untrained personnel and social engineering. These stories illustrated the importance of cybersecurity for public safety organizations and the need for improved cyber awareness and procedures within the public safety community.

Building on the discussion of experiences and challenges, the groups shifted to the draft Cybersecurity Primer and their impressions of the two resources presented during the panel, the NIST Framework and the Cybersecurity Framework. Many participants felt the primer should use a more urgent tone and include stories to highlight cybersecurity's importance. Other recommendations included providing actionable solutions to cyber issues, keeping the document simple and easy to understand, and drafting different versions for various audiences. Participant feedback on the Framework and Continuum were mixed, but overall positive. Most participants agreed that all three documents could be used to help stress the importance of cybersecurity for public safety organizations.

Funding and Sustainment

The Funding and Sustainment Committee utilized a joint break-out session to gather feedback on potential updates to the *2011 Emergency Communications System Lifecycle Planning Guide*. Members remained in their groups, and conducted facilitated discussions based on the six steps of the planning guide.

Table 1. Steps for System Lifecycle Planning

Step	Action (Timeline)	Goal
1	Planning (12-18 months)	Establish a formal planning team, identify all key elements of the affected system(s), and document the operational and technical requirements to support system replacement or upgrade.
2	Acquisition (12 months)	Leverage the Functional Requirements Document and use it to plan and prepare for the acquisition of the new system, and the development of procurement documents.

Table 1. Steps for System Lifecycle Planning

Step	Action (Timeline)	Goal
3	Implementation (12-18 months)	Get the system online, and up and running. The system has been procured and will be ordered, staged, installed, tested, and cutover (migrated). Once training is complete, the system will go live.
4	Support and Maintenance (10-15 years)	Ensure the accepted system stays at optimal operational level during its life
5	Refreshment (10-15 years)	Ensure the system continues to support the user's needs over the system's useful life
6	Disposition (90 days after cutover)	Ensure the old system components are disposed of without adverse impact to the operations of the new/upgraded system

Stakeholders held lively discussions on the planning timeline, personal experiences in lifecycle planning, and who should be involved in each step of the planning process. A majority of members felt that processes will be different for each state depending on current purchasing and acquisition guidelines. OEC and the Funding and Sustainment Committee will review the gathered data and begin updates to the Guide this summer.

EMERGENCY COMMUNICATIONS GOVERNANCE GUIDE

Charlie Sasser (National Association of State Technology Directors), Robert Symons (Wyoming SWIC), Dusty Rhoads, Kenzie Capece, and Miriam Montgomery, DHS, OEC, provided an update on the status of the *2015 Emergency Communications Governance Guide for State, Local, Tribal, and Territorial Officials* (2015 Governance Guide). The team sought feedback from SAFECOM and NCSWIC members to ensure that the Governance Guide includes comprehensive recommendations and best practices to establish or update emergency communications governance structures that holistically represent the emergency communications landscape. Mr. Rhoads noted that while much has been accomplished in the government-to-government lane of the emergency communications ecosystem (e.g., land mobile radio (LMR), broadband), the 2015 Governance Guide will ~~is~~ focus~~ed~~ primarily on strengthening the government-to-citizen lane and include the citizen-to-government lane.

Key benefits of the 2015 Governance Guide include:

- Providing insights into proven, repeatable models to improve statewide, intra-state, inter-state, local, tribal, and territorial emergency communications governance structures;
- Illustrating real-world examples for expanding or updating governance structures and processes to effectively address the evolving communications landscape; and
- Educating policy makers and elected officials on the importance of an effective governance body for collaboration and information and resource sharing to efficiently address emergency communications capabilities challenges.

To ensure support and input from stakeholders, OEC established the Governance Guide Working Group, chaired by Charlie Sasser, SAFECOM, and co-chaired by Penny Rubow, NCSWIC. Mr. Sasser explained that the Working Group includes SAFECOM and NCSWIC members, as well as other emergency communications governance subject matter experts. The Working Group has completed several critical activities in the process of developing the 2015 Governance Guide, including developing a detailed 2015 Governance Guide outline; identifying case study candidates based on their expertise and experience; completing governance profiles for more than 20 case study candidates; conducting discussion sessions with a majority of the 20 case study candidates; and defining characteristics, attributes, and activities of effective governance structures. The Working Group will assist with the development of the 2015 Governance Guide, validate findings, and review draft sections.

Case study candidates (Figure 3) were identified to provide a diverse perspective on governance structures. The 20 case study candidates were identified to analyze best practices and recommendations based on several factors, including geography, economic drives, governance structure authority, level of coordination across different communications capabilities, and population density. Case study candidates include representatives from 14 states, two regions, three cities, and one territory. The team conducted discussion sessions with selected case study candidates to understand complex conditions that make governance structures successful or challenging, and analyzed the information to identify key themes and best practices.

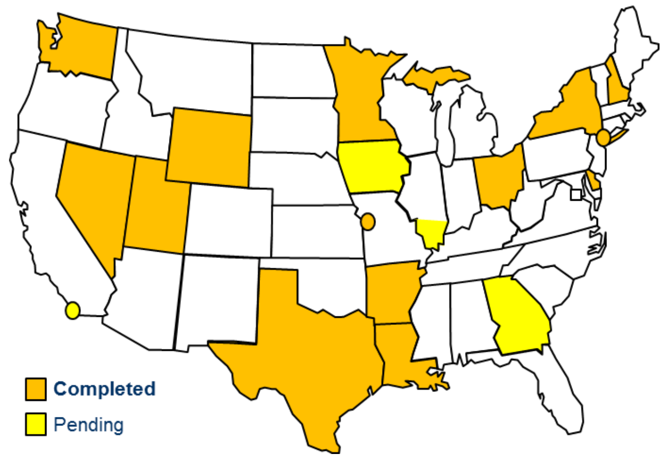


Figure 3. Case Study Candidates for the 2015 Governance Guide

After conducting discussion sessions with case study candidates, several high-level findings were identified, including:

- Types of Governance Authority:
  - EOs are enacted faster than legislation and provide governance bodies necessary authority; however, EOs may not survive gubernatorial elections because support is often dependent on the Governor's understanding and prioritization of emergency communications.
  - Legislation provides continuity in the face of government turnover at the state level; however, it often involves a lengthy process to make amendments.
  - Ad-Hoc authority is the most responsive type of authority to change because there is no requirement to obtain approval to adjust codified language; however, it is highly dependent on membership commitment.
- Governance Membership and Composition:
  - Appropriately sized membership is likely to lead to active participation.
  - Proper levels of authority help to advance initiatives and establish accountability.
  - Representation from different disciplines as well as having technical and functional expertise (e.g., police, fire, EMS, dispatcher) ensures users needs are adequately addressed and increases the likelihood of gaining buy-in from stakeholders.
  - Adequate representation at the state, territorial, local, and tribal representation increases the likelihood of shared responsibility and decision making across levels of government.
  - Personality plays an integral role in successful collaboration and coordination
  - Participation and accountability is important to ensure the member is an active participant and brings input from their constituents to the meetings and shares information from the Board
- Emergency Communications Landscape:
  - Emergency management agencies often oversee alerts and warnings capabilities without coordinating with the governance body.
  - 911/E911/NG911 coordination and governance typically occur at the local jurisdictional level with limited to no state-level involvement.
  - Broadband governance is typically integrated with LMR governance through the Statewide Interoperable Executive Committee (SIEC).
  - One of the main reasons LMR, broadband, and 911/NG911 capabilities are integrated under a single governance body or agency is the state's recognition of the convergence of emergency communications technology and operations.

- Recommendations for Identifying Funding Sources:
  - Establish state competitive grant programs with incentives for local jurisdictions to improve emergency communications capabilities
  - Leverage an entity that has pre-existing legislative authority to issue and administer bonds to reduce timeframe for public notice and approval
  - Limit reliance on "General Funds" for maintenance and operations of emergency communications capabilities because the funding level can fluctuate
  - Identify unique or creative funding sources based on the economic factors of the state or region (e.g., Louisiana Riverboat Gaming Fund, commercial entity financial donations)

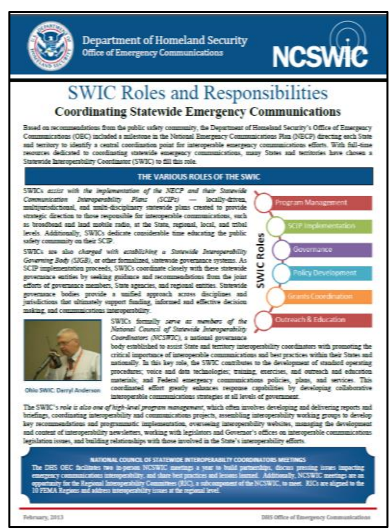
Steve Proctor noted that the Utah Radio System effectively utilizes a quasi-government entity, with a Board, created in response to the 2003 Olympics, made up of five state representatives and ten local representatives. Because the event proved to be the most successful event held in Utah, the same governance system exists today: one agency that coordinates all public safety needs. While it was a huge endeavor, establishing a governance body makes officials take an in-depth look at what is occurring in the state. Additionally, Mr. Proctor noted that Utah's legislature is planning to audit all 9-1-1 funds this year and is looking for a funding source to replace the statewide radio system.

When asked about how the state of Ohio built their governance model, Mr. Anderson noted that coordination began in the mid-1990s, with the creation of a statewide system. Looking back, he noted that the state should have tried to include the entire state in the system and to locate a funding source, similar to what Indiana accomplished through a license plate tax. Ohio worked with the SIEC to expand a platform for the statewide system and continued outreach at the local level. Mr. Anderson noted that a balanced partnership between state and local officials is key. Jim Goldstein (SAFECOM, International Association of Fire Chiefs) noted that certain states are better than others at getting local representatives involved, and agreed that building working relationships should be a priority.

There are between 5,800-7,000 PSAPs in use across the U.S., most of which are small facilities run by a local sheriff or police chief. PSAPs struggle to collaborate, especially across governance. Mr. Rhoads noted that governments cannot afford to have the number of governance structures necessary for coordinating PSAPs across the country, nor can that number of independent bodies successful operate. He stated the urgency for established governance prior to technology implementation. Regarding NG 9-1-1 in Ohio, Mr. Anderson noted that the state created a law resulting in PSAP consolidation aimed to improve efficiency and quality of services and response, responder safety, employee retention, and cost savings.

SAFECOM AND NCSWIC TOWN HALL

Chris Essid invited NCSWIC and SAFECOM members to participate in an open forum to discuss how OEC can improve stakeholder program support. Mr. Essid noted that OEC operates best when receiving direct feedback from its stakeholders and truly values member input. Mr. Essid encouraged attendees to engage with their peers in support of the value of these programs. Attendees noted that some of SAFECOM's associations still struggle to differentiate the missions and purpose of various public safety programs, and therefore, are still unsure of the value they or their products provide the community. Ralph Barnett, III, DHS, OEC, encouraged members to leverage the [SAFECOM website] and use existing outreach products, such as fact sheets, presentations, newsletters, monthly bulletins, and white papers to increase stakeholder education. George Molnar (SAFECOM, NCSWIC Vice Chair, Nevada SWIC) suggested that a one-page snap shot of the public safety environment would help SWICs address NCSWIC's importance and unique mission to government officials. Members agreed that future documents should use language that is easy to understand for those who are not familiar with industry terminology. OEC currently houses many stakeholder products


Department of Homeland Security
Office of Emergency Communications
NCSWIC

SWIC Roles and Responsibilities

Coordinating Statewide Emergency Communications

Based on recommendations from the public safety community, the Department of Homeland Security's Office of Emergency Communications (OEC) included a milestone in the National Emergency Communications Plan (NECP) directing each State and territory to identify a central coordination point for interoperable emergency communications efforts. With full-time resources dedicated to coordinating statewide emergency communications, many States and territories have chosen a Statewide Interoperability Coordinator (SWIC) to fill this role.

THE VARIOUS ROLES OF THE SWIC

SWICs *assist with the implementation of the NECP and their Statewide Communication Interoperability Plans (SCIPs)* — locally-driven, multijurisdictional, and multi-disciplinary statewide plans created to provide strategic direction to those responsible for interoperable communications, such as broadband and land mobile radio, at the State, regional, local, and tribal levels. Additionally, SWICs dedicate considerable time educating the public safety community on their SCIP.

SWICs are also *charged with establishing a Statewide Interoperability Governing Body (SIGB)*, or other formalized, statewide governance systems. As SCIP implementation proceeds, SWICs coordinate closely with these statewide governance entities by seeking guidance and recommendations from the joint efforts of governance members, State agencies, and regional entities. Statewide governance bodies provide a unified approach across disciplines and jurisdictions that ultimately support funding, informed and effective decision making, and communications interoperability.

SWICs formally *serve as members of the National Council of Statewide Interoperability Coordinators (NCSWIC)*, a national governance body established to assist State and territory interoperability coordinators with promoting the critical importance of interoperable communications and best practices within their States and nationally. In this key role, the SWIC contributes to the development of standard operating procedures; voice and data technologies; training, exercises, and outreach and education materials; and Federal emergency communications policies, plans, and services. This coordinated effort greatly enhances response capabilities by developing collaborative interoperable communications strategies at all levels of government.

The SWIC's *role is also one of high-level program management*, which often involves developing and delivering reports and briefings, coordinating interoperability and communications projects, assembling interoperability working groups to develop key recommendations and programmatic implementation, overseeing interoperability websites, managing the development and content of interoperability newsletters, working with legislators and Governor's offices on interoperable communications legislation issues, and building relationships with those involved in the State's interoperability efforts.

NATIONAL COUNCIL OF STATEWIDE INTEROPERABILITY COORDINATORS MEETINGS

The DHS OEC facilitates two in-person NCSWIC meetings a year to build partnerships, discuss pressing issues impacting emergency communications interoperability, and share best practices and lessons learned. Additionally, NCSWIC meetings are an opportunity for the Regional Interoperability Committees (RIC), a subcomponent of the NCSWIC, to meet. RICs are aligned to the 10 FEMA Regions and address interoperability issues at the regional level.

February, 2013 DHS Office of Emergency Communications

Figure 4. SWIC Roles and Responsibilites promotional document; published 2013

aimed at providing government officials with information on NCSWIC and SAFECOM programmatic missions, roles, and responsibilities (e.g., Figure 4), many of which are available on HSIN or will become available on the websites over the next few months.

As the public safety community continues to address new and emerging issues within the emergency communications ecosystem, attendees suggested that SAFECOM consider expanding its membership to technology-related organizations, railroad representatives, the United States Coast Guard, city managers, state legislators, and additional at-large membership. Attendees also discussed increasing partnerships with other federal organizations to increase coordination. Mr. Essid noted that the Emergency Communications Preparedness Center (ECPC) is a robust focal point for continuing interoperable and operable communications coordination. Steve Proctor and Harlin McEwen (SAFECOM, International Association of Chiefs of Police) are both non-voting members and regularly attendee its meetings.

Lastly, Mr. Symons asked that OEC stay aware of redundant projects. He explained that SWICs provide similar information on the NCSWIC Annual Report as they do to the Regional Emergency Communications Coordination Working Group (RECWG) Report. Mr. Essid noted that OEC is analyzing documents to avoid future duplication.

ATTENDEE ROSTER

NCSWIC

Name	State
Chuck Murph	Alabama
Matt Leveque*	Alaska
Jeremy Knoll	Arizona
Jack Cobb	Colorado
Michael Varney*	Connecticut
Mark Grubb*	Delaware
Jeff Wobbleton	District of Columbia
Phil Royce	Florida
Nick Brown*	Georgia
Brad Hokanson	Guam
Victoria Garcia*	Hawaii
Todd Herrera	Idaho
Russ Gentry (alternate)	Illinois
Steve Skinner	Indiana
Craig Allen*	Iowa
Jason Bryant*	Kansas
Derek Nesselrode	Kentucky
Ken Hasenei	Maryland
Brad Stoddard	Michigan
Sue Krogman	Nebraska
George Molnar*	Nevada
John Stevens	New Hampshire
Craig Reiner	New Jersey
Bernadette Garcia (alternate)	New Mexico
Robert Barbato*	New York
Jeffrey Childs	North Carolina
Michael Lynk	North Dakota
Darryl Anderson*	Ohio
Nikki Cassingham*	Oklahoma
Karl Larson (alternate)	Oregon
Mark Wrightstone	Pennsylvania
Felix Garcia*	Puerto Rico
Thomas Guthlein	Rhode Island
Robert Steadman*	South Carolina
Arnold Hooper (alternate)	Tennessee
Karla Jurrens (alternate)	Texas
Steve Proctor	Utah
Adam Thiel	Virginia
Bill Schrier (Alternate)	Washington
G.E. McCabe	West Virginia

Name	State
Gene Oldenburg	Wisconsin
Bob Symons*	Wyoming

***Denotes NCSWIC Executive Committee (EC) Member; all members are Statewide Interoperability Coordinators, unless otherwise noted*

SAFECOM

Name	Organization
Association Members	
Philip Mann	American Public Works Association
Gigi Smith*, Brent Lee*	Association of Public-Safety Communication Officials- International
Chris Lombard	Interagency Board
Harlin McEwen*	International Association of Chiefs of Police
Jim Goldstein*	International Association of Fire Chiefs
Scott Edson*, Christopher Cahhal*	Major Cities Chiefs Association
Mel Maier	Major County Sheriffs' Association
Bill Bamattre*	Metropolitan Fire Chiefs Association
Terry Hall*	National Association of Counties
Steve Cassano	National Association of Regional Councils
Bruce Cheney	National Association of State 9-1-1 Administrators
Darryl Ackley	National Association of State Chief Information Officers
Kevin McGinnis*, Paul Patrick*	National Association of State EMS Officials
Charlie Sasser	National Association of State Technology Directors
Robert Dickerson	National Association of Telecommunications Officers and Advisors
Richard Broncheau*	National Congress of American Indians
Mark Grubb*	National Council of Statewide Interoperability Coordinators
John Sweeney	National Criminal Justice Association
Jon Olson*	National EMS Management Association
Jimmy Gianato*	National Governors Association
Douglas Aiken*, Marilyn Ward*	National Public Safety Telecommunications Council
Paul Fitzgerald*, Larry Amerson*	National Sheriff's Association
Mike Jacobson	SEARCH, National Consortium for Justice Information and Statistics
Public Safety At-Large Members	
Don Bowers	Fairfaix County Fire and Rescue (Virginia)
Mark Buchholz	Willamette Valley 9-1-1 (Oregon)
Anthony Catalanotto	Fire Department City of New York (New York)
Len Edling	Merionette Park Fire Department (Louisiana)
Bradley Hokanson	Guam Homeland Security/Office of Civil Defense (Guam)
Jay Kopstein	New York State Division of Homeland Security and Emergency Services (New York)
Paul Leary	Department of Research and Economic Development (New Hampshire)

Name	Organization
Public Safety At-Large Members (continued)	
Michael Murphy	Many, Louisiana Police Department (Louisiana)
George Perera	Miami Dade Police Department (Florida)
Steve Proctor*	Utah Communications Authority (Utah)
Gerald Reardon*	City of Cambridge Fire Department (Massachusetts)
Thomas Roche	Monroe County, New York (New York)
Wes Rogers	Fairfax County Fire and Rescue (Virginia)
Bob Symons	Statewide Interoperability Coordinator (Wyoming)
Steve Verbil	Office of Statewide Emergency Telecommunications (Connecticut)
Brent Williams	Department of Community Health, EMS, and Trauma (Michigan)
Dan Wills	Arizona State Forestry (Arizona)

Denotes SAFECOM EC Member

FEDERAL PARTNERS

Name	Organization
Steve Noel, Tim Pierce	DOC, National Telecommunications and Information Administration (NTIA), First Responder Network Authority (FirstNet)
Gregory Boren, Brian Carney, Joanna Robichaud	Department of Homeland Security (DHS), Federal Emergency Management Agency (FEMA), Disaster Emergency Communications (DEC)
Rick Andreano, Ralph Barnett, III, , Robin Beatty, Ken Born, Ken Bradley, Billy Bob Brown, Kenzie Capece, Jim Downes, Chris Essid, Annie Glenn, Dan Hawkins, Jim Jarvis, Jessica Kaputa, Traci Knight, Ted Lawson, Jim Lundsted, Gabriel Martinez, Marty McLain, Pam Montanari, Miriam Montgomery, Dusty Rhoads, Adrienne Roughgarden, Dick Tenney, Chris Tuttle	DHS, Office of Emergency Communications (OEC)
Dan Cotter, Chris Espinosa	DHS, Office for Interoperability and Compatibility (OIC)

GUESTS

Name	Organization
John Contestabile	John Hopkins University
Barry Luke	National Public Safety Telecommunications Council