CSRIC V Working Group Descriptions and Leadership

CSRIC Chair
Chris Sambar, AT&T

Steering Committee Chair
Alyson Peacock, AT&T

Working Group 1– Evolving 911 Services

Co-Chair: Susan Sherwood, Verizon
Co-Chair: Jeff Cohen, APCO

FCC Liaisons: Tim May, John Healy

Description: Advancements in wireless devices (operating systems and application platforms) and licensed and unlicensed wireless networks have led to the rapid development of commercial location based services. Today, however, when a 911 call is initiated, in order to determine the proper Public Safety Answering Point (PSAP) to which to route the call, wireless service providers use the cell sector of the cell site or base station that received the call. Current industry standard practice requires that these 911 call routing arrangements be pre-agreed between the carrier and the PSAPs within or near the coverage area of the cell site/sector, with a single PSAP instructing the carrier which given cell site/sector they should receive 911 calls from. In many instances, cell sector coverage areas can cover more than one PSAP jurisdiction, leading to transfers of calls between PSAPs and potentially slowing emergency response times. PSAPs have existing best practices and standard operating procedures in place to transfer calls to another PSAP, and this is especially true when this is a common occurrence such as when a cell sector is covering a state border. Thus the main cause of the need for PSAPs to transfer calls is due to the physical characteristics of radiofrequency transmissions, which do not respect jurisdictional borders. In some instances, neighboring jurisdictions lack geographical information necessary to properly reroute a call. Location-based routing may offer the ability to more quickly and accurately route 911 calls to the appropriate PSAP.

Task 1: Working Group 1 will review public safety and industry best practices and standard operating procedures for rerouting 911 calls between PSAPs resulting from the use of cell sectors for routing purposes, and where necessary identify gaps and make recommendations towards mitigating PSAP call transfers and optimizing rerouting best practices. The review should include an analysis of the inter-jurisdictional coordination necessary to ensure that Master Street Address Guides (MSAG) and Geographical Information Systems (GIS) cover all areas where cell sector coverage may lead to the routing of a 911 call to the incorrect jurisdiction. In addition, the Working Group should assess whether current best practices and standard operating procedures address call transfer and rerouting issues associated with the deployment of Emergency Services IP networks (ESInets) that handle 911 calls for multiple jurisdictions operating in partnership but which may not incorporate PSAPs bordering the regional partnership.

Task 2: Working Group 1 will study and make recommendations on the architectural, technical, operational standards, and cybersecurity requirements of location based routing that uses longitude and latitude information or other location identification methods (when available) to determine and route a 911 call to the nearest appropriate PSAP. In addition, the Working Group will explore and report on the pros and cons of various sources of location information available for location-based routing, the potential reliability and accuracy of the sources, and the transition path to location-based routing of 911 calls from legacy to hybrid and then fully deployed Next Generation 911 systems, in particular identifying the

necessary roles and responsibilities of key stakeholders involved in supporting 911 calls and identify existing and future standards to support the transition.

Milestones:
1. Task One - Report and Recommendations - March 2016.
2. Task Two - Report with Guidelines and Recommendations - September 2016.

Working Group 2 – Emergency Alerting Platforms

Co-Chair: Francisco Sanchez, Harris County (TX) Office of Homeland Security & Emergency Management
Co-Chair: Farrokh Khatibi, Qualcomm

FCC Liaisons: Chris Anderson, James Wiley, Gregory Cooke

Description: This Working Group will review WEA security practices and recommend any actions, including the development of best practices, that the Commission should take to improve WEA security. Such review and recommendations shall include an examination of how the integrity of the C-interface can be protected, how to protect against the exploitation of vulnerabilities in carrier networks and in the practices and operations of State and Local Emergency Management systems, and how WEA message data can be protected on cellular handsets. In this regard, the Working Group should take into consideration new and evolving technologies that may reduce cyber risks to WEA networks and services.

Further, the Working Group will provide recommendations on how best to encourage the use of emergency alerts by state and local officials at a local/geo-targeted level, including leveraging different alerting platforms and the coordination of information flow from both "one-to-many" and "many-to-one". The Working Group would also discuss and provide recommendations on technical issues such as (a) how public safety officials can leverage various platforms (including commercial alerts/social media) to best alert the public while enabling the public to share information back with public safety officials; and (b) the technical opportunities/barriers to coordinating multiple alerting platforms, as well as the development of standards that could result in improvements to public safety outcomes.
The Working Group will consider the use of "many-to-one" methods for Public Safety officials to rapidly receive and accumulate feedback from the public concerning developing incidents.

Milestones:
1. Recommendation to the Commission on WEA Security – March 2016.
2. Wireless Emergency Alerts: Recommendations to Improve Geo-Targeting and Offer Many-to-One Capabilities – September 2016
3. Social Media & Complementary Alerting Methods: Recommended Strategies & Best Practices – September 2016

Working Group 3 - Emergency Alert System

Co-Chair: Steven Johnson, Johnson Telecom
Co-Chair: Kelly Williams, NAB

FCC Liaison: Gregory Cooke

Description: This Working Group will make recommendations to the Commission in three major areas related to the continued improvement and development of the EAS as a secure, effective alerting tool for the American public: EAS Security, the provision of EAS in languages other than English, and the development of an operational handbook for individual broadcasters, cable service providers and other EAS Participants.

EAS Security - The working group will make recommendations concerning the implementation of the EAS cyber security best practices adopted by the CSRIC III. Subsequent to the CSRC's adoption of these best practices, the Commission had released a public notice in which it sought comment on the extent to which these best practices had been adopted. The Commission intends to initiate a rulemaking in the 4th quarter of 2015 that will address EAS security issues and the response to the initial Public Notice has been not been sufficient to allow the Commission to build an informative record. Accordingly, the working group will present its recommendations to the CSRIC for the CSRIC's adoption at its fall 2016 meeting. Any recommendations adopted by the CSRIC will be incorporated into the record of that proceeding. Specifically, the working group will assess any barriers to the adoption of the CSRIC III best practices, and will make recommendations on incentives, both regulatory and non-regulatory for affected stakeholders to adopt the best practices. The working group will also recommend methods by which other EAS stakeholders may gain assurance that the best practices are being implemented.

Multilingual EAS - The Working Group will recommend best practices for the delivery of multilingual EAS and emergency information. The Working Group will pay particular attention to how communities determine their multilingual needs, and how individual broadcasters, cable service providers and other EAS Participants (including rural, smaller and less resourced EAS Participants) and their representative organizations address those needs. Areas of interest should include specific technical options ranging from having translators on staff to state of the art translation software. The Working Group will keep in mind how these practices can be expanded to include other communities that require enhanced access such as those with disabilities and the functional-needs community.

Updating the EAS Operating Handbook - According to section 11.15 of the Commission's rules, all EAS Participants must have a copy of the EAS Handbook located at normal duty positions or EAS equipment locations when an operator is required to be on duty and be immediately available to staff responsible for authenticating messages and initiating actions associated with the EAS process. According to the rules, the EAS Operating Handbook states in summary form the actions to be taken by personnel at EAS Participant facilities upon receipt of an EAN, an EAT, tests, or State and Local Area alerts. It is issued by the FCC and contains instructions for the above situations.

The current handbook is obsolete and contains inaccurate instructions. The Working Group will analyze the manner in which the EAS should operate and each type of EAS Participant (e.g., broadcaster and cable service provider facilities) and shall make recommendations for textual and visual elements of a handbook suitable for each category of EAS Participant, with particular attention to be given to rural, smaller and less resourced EAS Participants.

Milestones:

1. Recommendation to the Commission on EAS Security – March 2016.
2. Recommendation to the Commission on Multilingual EAS – September 2016.
3. Recommendation to the Commission on Draft EAS Handbooks – June 2016.

Working Group 4 – Communications Infrastructure Resiliency
Sub-Group A: Submarine Cable Resiliency

Co-Chair: Kent Bressie, North American Submarine Cable Association
Co-Chair: Catherine Creese, US Naval Seafloor Cable Protection Office

FCC Liaisons: Michael Connelly, Jerry Stanshine

Description: Submarine cable resiliency is essential for U.S. economic and security interests, as submarine cables provide the majority of U.S. international connectivity and significant domestic connectivity for certain U.S. states and territories. At present, however, several factors, including the expense and time requirements for permitting of new cable stations, other shore-end facilities, and terrestrial backhaul often encourages new cable landings using existing landing facilities. Moreover, increasing authorization and development of alternative energy facilities near submarine cable facilities could foreclose submarine cable routing and landing in particular marine and shore areas.
The working group shall recommend industry practices, government policies, and interagency coordination mechanisms to promote a more resilient submarine cable infrastructure. For example, it will develop recommendations for enhancing coordination amongst federal, state and local agencies and also recommend ways the Commission can work with other agencies to ensure submarine cable resiliency. In doing so, the working group shall take into account the Commission's statutory jurisdiction under the Cable Landing License Act and the Communications Act and the existing interagency coordination process established in Executive Order 10,530.

Milestones:
1. Recommendations for enhancing coordination between and among federal, state, and local agencies without increasing regulatory burdens –June 2016.
2. Recommendations for promoting geographic diversity of routes and landings - September 2016.

Sub-Group B: Network Timing Single Source Risk Reduction

Chair: Jennifer Manner, EchoStar

FCC Liaison: Emil Cherian

Description: Synchronized network timing is a crucial element of communications network management. For call handoffs to take place between cell sites or for time-division multiplexing, components of a communications network need to be aligned to a trusted, precise network timing source. The communications sector relies heavily on GPS to provide network time. GPS is a widely available, extremely precise timing source that is used across multiple infrastructure sectors. However, given the high dependence of the communications sector on GPS, the Commission is interested in identifying ways to increase the resilience of communications networks by exploring complementary or backup solutions that could be employed to offer similar time precision as GPS in the event that GPS signals are lost. These solutions also need to be completely independent of GPS to truly reduce risk. The working group will assess current options and technologies that meet these criteria that could be employed across the sector.

The group will be informed by DHS work in this area. They will study business resiliency needs related to private sector, commercial and consumer needs.

Milestones:
1. Report on options on acquiring and implementing backup precision timing solutions that are independent of GPS and submission of WG4B Report 1 on Options - June 2016.
2. Report on recommendations on acquiring and implementing backup precision timing solutions that are independent of GPS and Submission of Final WG4B Report - December 2016.

Working Group 5 – Cybersecurity Information Sharing

Co-Chair: Rod Rasmussen, InfoBlox
Co-Chair: Christopher Boyer, AT&T

FCC Liaisons: Greg Intoccia, Vern Mosley

Description: To improve the communication sector's ability to identify, protect, detect, respond, and recover from cyber attacks, Working Group 5 will develop recommendations to the Commission to encourage sharing of cybersecurity information between companies in the communications sector. These recommendations will offer guidance on how communications companies can effectively share cyber risk information pertinent to communications critical infrastructure within the private sector. The cybersecurity information under consideration will include: (1) non-real-time threat indicators and warnings, (2) real-time anomalous indicators, and (3) post-incident information related to cyber attacks on communications critical infrastructure as described in the CSRIC IV Working Group #4 report.. WG5 will organize into four study efforts: (1) Use Cases, (2) Information Sharing Barriers, (3) Information Sharing "Trust Pools," and (4) Conduits for Information Sharing. Each of the efforts is described below.

Use Cases. This effort will document and/or develop a cybersecurity information sharing baseline of what the industry is doing today including examples of current and prospective use cases that address the sharing of (1) non-real-time threat indicators and warnings, (2) real-time anomalous indicators, and (3) post-incident information related cyber attacks on communications critical infrastructure across the communications sector. The identified Use Cases will be used to inform the work of other groups to develop their recommendations.

Information Sharing Barriers and Solutions. This effort will identify and assess perceived technical, legal, financial, consumer/market, operational, and/or organizational impediments to cyber threat information sharing and/or the implementation of the prospective use cases, analyze potential solutions to the impediments, and develop recommendations that would enable cybersecurity information to be broadly shared across the communications sector. Barriers and potential solutions will be examined in sharing cybersecurity information (threat indicators and warnings, anomalous indicators, and post-incident information) between private entities.

Optimal Sharing "Trust Pools": This effort will identify, assess, analyze, and develop recommendations for how industry engages with information sharing "trust pools" that presently exist (e.g. NCC), or may be developed pursuant to the Administration's recent information Executive Order establishing Information Sharing and Analysis Organizations (ISAOs).

Conduits for Information Sharing: This effort will identify and assess structures and platforms for the communications sector stakeholders to routinely share cybersecurity information (threat indicators and warnings, anomalous indicators, and post-incident information) within the constraints of existing law.

Milestones:
1. Cybersecurity Information Sharing Diagram – December 2015.
2. Baseline and Draft Use Cases – January 2016.
3. Final Use Cases – March 2016.

4. Technical/Legal/Financial/Consumer/Market/Operational/Organizational Impediments/Barriers and Solutions to Cybersecurity Information Sharing - June 2016.
5. Cybersecurity Information Sharing "Trust Pools" - September 2016.
6. Cybersecurity Information Sharing Platforms - December 2016.
7. Recommendations for Cybersecurity Information Sharing - March 2017.

Working Group 6 - Secure Hardware and Software – Security by Design

Co-Chair: Brian Scarpelli, ACT The App Association
Co-Chair: Joel Molinoff, CBS

FCC Liaisons: Steven McKinnon, Emily Talaga

Description: In order to enhance the security of hardware and software in the core public communications network, Working Group 6 will provide recommended capabilities to better ensure the security of the supply chain for critical communications infrastructure. The supply chain consists of several distinct segments: design and development, distribution, and maintenance; each of which has its own risks and vulnerabilities.

These recommended capabilities may make use of security by design principles and processes that should allow network equipment manufacturers to make the core communications network more secure, resilient, and defendable from Internet-based attacks.

The recommendations will be guided by the recommendations developed by the FCC's Technology Advisory Council (TAC) on December 4, 2014. Potential outcomes could include, but are not be limited to, recommended capabilities for network equipment default settings when used within ISP networks (e.g., source address validation as a default to reduce spoofing), review of network connected devices running communications protocols vulnerable to DDoS amplification attacks (e.g., Simple Service Discovery Protocol (SSDP) enabled as a default setting), and reviewing how the Commission, and more broadly the federal government, could look to promote and encourage the use of standards enhancing both network security and performance (e.g., the use of Unicast Reverse Path Forwarding (uRPF) mode on all network routers purchased by the federal government).

In the course of its work, Working Group 6 should work closely with standards organizations like 3GPP and ATIS to direct attention to the existing standards that would be most useful when applied to security by design principals as applied to core network equipment. In addition, Working Group 6 should examine and review the best ways of providing assurances to the FCC and the public that these recommended security capabilities are being implemented by network equipment vendors.

Milestones:
1. Prepare and present recommendations for the security best practices that network equipment suppliers should follow – March 2016.
2. Recommend voluntary mechanisms that provide assurances to the FCC and the public that the recommended security best practices are being applied – September 2016.

Duration: 1 year

Working Group 7 - Cybersecurity Workforce

Chair: Bill Boni, T-Mobile

Alternate Chair: Drew Morin, T-Mobile

FCC Liaison: Erika Olsen

Description: This working group will examine and develop recommendations for the CSRIC's consideration regarding any actions that the FCC should take to improve the security of the nation's critical communications infrastructure through actions to enhance the transparency, skill validation, and best practices relating to recruitment, training, retention, and job mobility of personnel within the cybersecurity field. Specifically, this working group will leverage existing work in the context to enhance the volume and quality of the workforce, including: (1) demonstrating the application of the NICE Cybersecurity Workforce Framework (CWF) to the common and specialized work roles with in the communications sector; (2) identifying any gaps or improvements in the CWF for evolving work roles or skill sets that should be included in sector members' workforce planning; and (3) identifying, developing and recommending best practices and implementation thereof to mitigate insider threats, including through scalable means to enhance transparency, accountability and validation of skills, knowledge and abilities within the communications sector and particularly with respect to personnel having access to the most critical elements of the nation's communications network assets. In this respect, the working groups should consider means to promote a common lexicon and roadmap that will promote more effective interface with academic institutions and other training environments.

Milestones:

1. Demonstrate the application of the NICE Cybersecurity Workforce Framework (CWF) to the common and specialized work roles with in the communications sector - March 2016.
2. Identify any gaps or improvements in the CWF for evolving work roles or skill sets that should be included in sector members' workforce planning - March 2016.
3. Identify, develop and recommend best practices and implementation thereof to mitigate insider threats within the communications sector including through scalable means to enhance transparency, accountability and validation of skills, knowledge and abilities, particularly with respect to personnel having access to the most critical elements of the nation's communications network assets. - March 2017.

Working Group 8 – Priority Services

Chair: William Reidway Jr., Neustar, Inc.

FCC Liaisons: Tim Perrier, Ken Burnley

Description: Priority communications over commercial networks during a national emergency remains as essential today to responders and national security personnel as in decades past. However, commercial communications networks are increasingly relying on packet-based technology and retiring Time Division Multiplexing (TDM) technology. The Federal government is losing priority capabilities throughout this transition, as voice priority services rely on wireline TDM, which will eventually be replaced by IP-based infrastructure. Lack of priority communications services on packet-based systems could jeopardize national security or domestic incident response.

Further, as advances in command-and-control focus increasingly on the transmission of rich data content, such as real-time streaming video, programs established by the government originally to ensure availability and access to voice communications could take advantage of the additional capabilities that packet-based networks can provide. In addition, the transition from IPv4 to IPv6 may offer opportunities to increase performance, security and privacy, and authentication mechanisms.

The working group will assess how priority services programs can take advantage of packet-based technologies and recommend protocols that can be used to ensure priority communications upon retirement of TDM. The working group also should incorporate the impact of the IPv6 transition into its recommendations.

Milestones:
1. Draft WG8 Report 1 - June 2016.
2. Draft WG8 Report 2 - Sept 2016.
3. Final WG8 1 Report - December 2016.
4. Final WG8 Report 2 - March 2017.

Working Group 9 – Wi-Fi Security

Chair: Brian Daly, AT&T

FCC Liaisons: Peter Shroyer, Kurian Jacob

Description: This Working Group will develop, for CSRIC's consideration, recommended best practices for promoting security in networks and devices utilizing Wi-Fi spectrum bands. Security concerns threaten entities utilizing Wi-Fi devices and spectrum. Currently, enterprises utilizing Wi-Fi spectrum rely on numerous methods to secure their networks and connected devices from malicious attacks. Working Group 9 will identify, for CSRIC's consideration when, and under what circumstances, the use of a variety of advanced security techniques are appropriate. Specifically the Working Group will identify, for CSRIC's consideration: 1) the threats most consistently facing Wi-Fi network operators and users; 2) the available security techniques to prevent and/or remediate the threats; 3) the extent to which each technique is effective against specific threats, avoids interference with legitimate activity, is easily deployed, and is currently deployed.

Milestones:
1. Prepare and present recommended security best practices for Wi-Fi operators, users, and consumers. – March 2017.

Working Group 10 – Legacy Systems and Services Risk Reduction
Co- Chair: John Kimmins, iconectiv
Co-Chair: Danny McPherson, Verisign
FCC Liaison: Steven McKinnon

Description: In the Technology Transitions Order in August 2015, the Commission notes that "communications are rapidly transitioning away from" TDM-based technologies to "new, all-IP multimedia networks." The intermingling of legacy communications technologies with advanced communications technologies introduces new threat vectors and cyber risk. For example, TDM-based vulnerabilities continue to highlight the need for increased awareness of and focus on improved security in legacy technologies even as those technologies enter their sunset phase. Recently, this issue has become an even greater problem area in light of the security vulnerabilities exploited and documented with Signaling System 7 (SS7), a signaling protocol supporting call setup, routing, exchange, and billing functions in communications networks by sending messages between fixed and mobile communications service providers. The scale of SS7, which is used by carriers all over the world, means that every network subscriber could be vulnerable to these security risks.

In one of what we expect will be a series of requests to CSRIC, the Commission asks CSRIC to examine vulnerabilities associated with the SS7 protocol. We are concerned that SS7 is subject to the loss of confidential data and disruption of communications services. These security vulnerabilities can also have an impact on the migration from legacy technologies and protocols like SS7 to IP-based protocols and technologies such as VoIP. Communications providers have been exploring ways to prevent exposure of network data traffic to malicious actors. This CSRIC Working Group will assess vulnerabilities and current defensive mechanisms and make recommendations to the FCC on how to overcome security challenges present in SS7 and other legacy communications protocols and their impact on the transition to next generation networks. Specifically, the Working Group is asked to consider and address the following questions:

1. How and why is SS7 vulnerable to cyber exploit? How do these or similar vulnerabilities impact newer technologies and protocols (e.g., SIP, IP)?
2. How can SS7 exploits lead to disruptions to communications and data loss? Are there vulnerabilities present in other network elements and protocols interfacing with SS7 (e.g., DSLAMS, Session Border Controllers, etc.)?
3. Would a compromise in SS7 put interconnected broadband networks at risk for confidentiality, integrity, and availability of network data?
4. What best practices and mitigation strategies exist to mitigate these risks? Are these best practices and mitigation efforts sufficient and being applied universally?
5. Given the most likely threats, where do risk mitigation efforts need to be applied in the near-term?
6. Are there unique threats to SS7 signaling in the U.S. from interconnected SS7 vulnerabilities? In what manner are these risks being mitigated today and are there additional controls that should be considered?
7. What other network interfaces could be impacted by SS7 exploits? For example, how could the interface between domestic and international mobile networks be vulnerable to SS7 exploits? How could the relationships between service providers and third party signaling vendors be vulnerable to SS7 exploits?

Milestones:
1. Preliminary Risk Assessment and Summary Report – September 2016.
2. Final Report with Risk Mitigation Recommendations – March 2017.