CSRIC VI Working Group Descriptions

Working Group 1: Transition Path to NG911

Chair: Mary Boyd, West Safety Services
FCC Liaison: John Healy

Description: The nation's transition from legacy 911 circuit switched network routers and call handling platforms to NG911 IP-based emergency services IP-networks (ESInets) and core services presents the opportunity to assess the reliability and resiliency of the networks and functional elements supporting the transition. The FCC directs CSRIC to recommend measures to improve both legacy 911 and NG911 systems, to include recommending ways in which the FCC may further the NG911 transition and enhance the reliability and effectiveness of NG911 through routing redundancy and maintenance and mitigate against the threat of outages to both legacy 911 and NG911 systems. The FCC also directs CSRIC to recommend actions the FCC could take to encourage the private sector to detect or deter threats to 911 before they reach the ESINet perimeter. The focus would be on identifying tools that are already available or not burdensome to implement, and on developing a set of best practices for carriers and 911 service providers. In addition, the FCC directs CSRIC to advise the FCC on small carrier issues related to NG911 implementation, including recommendations on how the FCC could address these issues. This would include advice on what small carriers in the state or region need to do to be ready on time to deliver their 911 traffic in an NG911-compatible manner; what economic disadvantages, if any, may impede small carriers in implementation of NG911; and what barriers to implementation, if any, the FCC should address. The FCC would ask CSRIC to recommend a "NG911 readiness checklist" for small carriers analogous to the one Task Force on Optimal Public Safety Answering Point Architecture (TFOPA) developed for PSAPs.

***Task 1 – 911 System Reliability and Resiliency during the NG911 Transition*:** The Working Group will review existing best practices and develop additional guidance regarding overall monitoring, reliability, notifications, and accountability in preventing 911 outages in transitional NG911 environments. In particular, the Working Group will identify risks associated with transitional 911 systems that could result in disruptions to 911 service and make recommendations to protect them, including recommendations for best practices and standards development The Working Group will study specific actions that originating service providers, 911 system service providers and other entities in the 911 call chain should take to detect and deter outage precursors before 911 calls are delivered to the ESInet gateway.

***Task 2 - Small Carrier NG911 Transition Considerations*:** The Working Group will study and develop recommendations for the CSRIC's consideration on small carrier best practices for managing the transition to NG911. This would include advice on what small carriers operating within a state region need to do to be ready on time to deliver

their 911 traffic in an NG911-compatible manner; what economic disadvantages, if any, may impede small carriers in implementation of NG911; and what barriers to implementation, if any, the FCC should address. The FCC directs CSRIC to recommend a "NG911 readiness checklist" for small carriers analogous to the one TFOPA developed for PSAPs.

***Milestones**:*

1. Report on 911 System Reliability and Resiliency during the NG911 Transition - June 2018.
2. Report on Small Carrier NG911 Transition Considerations – September 2018.

Working Group 2: Comprehensive Re-imagining of Emergency Alerting

Chair: Farrokh Khatibi, Qualcomm
FCC Liaisons: Steven Carpenter and Austin Randazzo

***Description*:** The Commission directs CSRIC to conduct a comprehensive evaluation of emergency alerting and emerging technologies (such as the ATSC 3.0 broadcast standard and 5G) that may result in new alerting capabilities. As part of this evaluation, this Working Group would develop recommendations for CSRIC's consideration on ways to streamline, simplify (by reducing burdens on licensees), and modernize existing systems, including the Emergency Alert System (EAS). This Working Group will review the processes and requirements for the EAS and related systems, and develop recommendations for CSRIC's consideration regarding any necessary technical protocols and processes to improve the reliability of emergency alerts by strengthening the authentication and integrity of these systems, including the EAS. As part of this overall evaluation, this Working Group develop recommendations on any technical solutions to support authentication of alerts through digital signatures for both the Internet-based IPAWS and the broadcast-based legacy "daisy chain" to ensure that the alert retransmitted by an EAS Participant was generated by an authorized alert originator and has not been modified since its generation. This Working Group also will examine whether any amendments or changes to existing technical protocols (including the Commission's rules or existing technical standards) are necessary to ensure the alert is only retransmitted during its valid period (e.g., during its current year, day, and time) and, if so, provide corresponding recommendations.

Milestones:

1. Report on Reimagining Alerting – June 2018.
2. Report on Authentication and Validation – December 2018.

Working Group 3: Network Reliability and Security Risk Reduction

Chair: Travis Russell, Oracle
FCC Liaison: Vern Mosley

Description: The FCC directs CSRIC to recommend mechanisms to reduce risks to network reliability and security, including: (i) best practices to mitigate the network reliability and security risks associated with the Diameter protocol, an industry standard for connecting and authenticating subscribers on mobile networks, (ii) mechanisms to best design and deploy 5G networks to mitigate risks to network reliability and security posed by the proliferation of Internet of Things devices, vulnerable supply chains, and open-source software platforms used in 5G networks, and (iii) best practices and tools to improve reliability and reduce security risks in IP-based networks and protocols.

The working group will identify and examine the security risks to wireless protocols (e.g., Diameter) impacting network reliability. Once the security risks have been identified and examined for their impact on network reliability, the working group will propose to CSRIC recommendations, including best practices, to mitigate the identified risks.

The working group will also identify and examine the security risks to the emerging 5th generation wireless networks including risks associated with the proliferation of the Internet of Things (IoT) endpoints, vulnerable supply chains, open-source 5G software platforms (e.g., OpenStack), network function virtualization (NFV), and software defined networking (SDN). Once the security risks have been identified and examined for their impact on network reliability, the working group will develop recommendations for CSRIC's consideration regarding best practices for the design, deployment, and operation of risk-tolerant 5G networks to mitigate the identified risks.

Lastly, the working group will identify and examine the security risks presented by IP-based protocols as they are used within the commercial communications infrastructure, and propose recommendations, including best practices to mitigate these risks. The examination should include risks inherent to Border Gateway Protocol, the protocol responsible for routing of IP-based communications traffic, and Domain Name Server, the utility that associates names with routable IP addresses.

Milestones:

1. Report on Best Practices and Recommendations to Mitigate Security Risks to Wireless Protocols – March 2018.
2. Report on Best Practices and Recommendations to Mitigate Security Risks to Emerging 5G Wireless Networks – September 2018.
3. Report Best Practices and Recommendations to Mitigate Security Risks to Current IP-based Protocols – March 2019.