

## **CSRIC IV Working Group Descriptions and Leadership**

**CSRIC Chair**  
**Larissa Herda**  
**CEO – TW Telecom**

**Steering Committee Chair**  
**Mike Rouleau**  
**TW Telecom**

### **Working Group 1– NG911**

**Co-Chair – Brian Fontes - NENA**  
**Co-Chair – Laurie Flaherty - NHTSA**  
**FCC Liaison – Tim May**

#### **Description:**

#### **Tasking 1 – Text-to-911**

In March 2013, ATIS/TIA adopted the Joint ATIS/TIA Native SMS to 911 Requirements and Architecture Specification defining the requirements, architecture, and procedures for text messaging to 911 emergency services using native wireless operator texting capabilities for the existing generation and Next Generation 911 PSAPs. The standard, however, does not address the following areas, which may be the subject of the ongoing text-to-911 rulemaking.

1. **Location Determination:** The ATIS/TIA standard specifies the provision of cell site and sector location information. The Working Group will study and report on the technical feasibility for wireless carriers to include E911 Phase 2 location accuracy and information in texts sent to 911 and make recommendations for including enhanced location information in texts to 911.
2. **PSAP Requests for Service:** In March 2013, ATIS and TIA released the Joint Native SMS-to-911 Requirements and Architecture Specification. The standard assumes that a PSAP will designate the text to 911 delivery method to the PSAP, including type of delivery method, or an alternate PSAP (and method) that will accept messages on behalf of the PSAP, or the PSAP will indicate that text-to-911 is not supported at all. The ATIS/TIA standard does not provide a mechanism for supporting this functionality and indicates that it is an area of future study. In the May 2013 Report & Order on Text-to-911 establishing bounce-back requirements on covered text providers, the FCC requires wireless carriers to provide a mechanism for PSAPs to notify the carrier to temporarily suspend text-to-911 service and to restart text-to-911. The Working Group will recommend best practices, including testing and trialing, operational procedures, and security requirements that wireless carriers, Public Safety Answering Points (PSAPs),

and third party service providers should follow in provisioning PSAP requests for text-to-911 service.

### **Tasking 2 – Location Accuracy and Testing for Voice-over-LTE Networks**

Current FCC location accuracy requirements under 20.18(h) permit network-based carriers to begin “blending” their GPS handset-based location data with their network-based data at the different benchmarks between January 2012 and January 2019. Based on the CSRIC III recommendations in the WG3 March 2012 Report for certain key performance indicators (KPIs) and the different types of empirical testing as part of the recommended maintenance testing every two years, the Working Group will examine whether those recommendations still apply for network-based carriers reconfiguring to Voice over LTE (VoLTE) platforms. They will examine any necessary changes in the testing recommendations and recommend cost efficient measures to meet the current location accuracy parameters in 20.18. Also, the Working Group will examine the capabilities of VoLTE reconfigured networks to provide enhanced location capabilities and consider methodologies to resolve the differences in opinions on location performance and “yield” referred to in Part 7 of the March 2012 Report.

### **Tasking 3 – Specification for Indoor Location Accuracy Test Bed**

In its Indoor Location Test Bed Report, CSRIC III WG3 recommended that the Commission charter future stages of the test bed under the auspices of future CSRIC working groups in order to continue the assessment of current and evolving location technologies. CSRIC III WG3 found that “several cycles of testing, at regular intervals, are needed to support the rate of technology development” and that “a test bed management structure with contractual authority that extends beyond [CSRIC] cycles will encourage ongoing technology development.” The Working Group, therefore, will examine the requirements to establish a permanent entity to design, develop, and manage an ongoing public test bed for indoor location technologies that can provide the FCC with regular comprehensive, unbiased and actionable data on the efficacy of location technologies. The Working Group will consider chartering requirements, including prerequisites for impartial test bed administration and maintenance of data confidentiality; types of entities that could assume the role as test bed administrators; technical requirements; scope and scale of necessary facilities and locations; permanent or contracted human resources to manage the test bed; start-up and ongoing cost requirements to maintain the test bed on an ongoing basis; and other considerations necessary to establishing an independent testing administrator.

#### **Duration:**

- 1.

## **Working Group 2 – Wireless Emergency Alerts**

**Co-Chairs – Brian Josef – CTIA**

**Co-Chairs – John Madden – NEMA**

**FCC Liaisons – Eric Ehrenreich, Julia Tu**

**Description:** This Working Group will review the Commission’s current Wireless Emergency Alert (WEA) rules, taking into account: (1) experiences with WEA since its deployment on April 7, 2012 (including those of WEA industry participants, the Federal Gateway and alert originators), (2) technological advances since the original WEA technical recommendations were submitted by the Commercial Mobile Service Alert Advisory Committee in 2007, and (3) other factors, as appropriate, and develop recommendations for CSRIC’s consideration for any necessary changes to ensure that WEA continues to serve as a valuable method to alert the public during an emergency. Such review shall include, but is not limited to, examination of issues such as geographic targeting, testing, message content and character limitation, other potential types of WEA alerts such as audio streaming, video streaming and multimedia, accessibility of WEA alerts to people with disabilities and those who do not speak English, and security. `

### **Duration:**

- 1.

## **Working Group 3 – EAS**

**Co-Chair – Larry Walke, NAB**

**Co-Chair - Clay Freinwald, Washington State**

**FCC Liaison – David Munson**

**Description:** This Working Group will develop recommendations for the CSRIC's consideration regarding any actions the FCC should take to improve the Emergency Alert System (EAS). Specifically, the Working Group will review the FCC's rules regarding state EAS plans and recommend any actions, including best practices, the Commission should take to improve the process for State Emergency Communications Councils’ (SECCs) development of and submission of plans as well as the FCC's process of review and approval of such plans. In this regard, the Working Group shall take into consideration the transition to the Common Alerting Protocol. The Working Group will also develop recommendations for any actions, including best practices, the Commission should take to promote the security of the EAS. The Working Group will address such other EAS-related issues as assigned to CSRIC by the FCC.

**Duration: WG should submit its recommendations for state EAS plans within 4 months of CSRIC’s first meeting.**

- 1.

#### **Working Group 4 – Cybersecurity Best Practices**

**Chair – To be named later**

**FCC Liaison –**

**Description:** The last set of comprehensive cybersecurity best practices was recommended by CSRIC in March 2011. In the time that has passed, the state of the art in cybersecurity has advanced considerably. This Working Group will update the best practices last produced by CSRIC II Working Group 2A.

**Duration: 12 months (February 2014 – March 2015)**

1.

#### **Working Group 5 – Remediation of Server-Based DDoS Attacks**

**Co-Chair – Pete Fonash, CTO DHS**

**Co-Chair – Mike Glenn, CenturyLink**

**FCC Liaison – Vernon Mosley**

**Description:** Critical infrastructure sectors, including the financial sector, have been under assault from a barrage of DDoS attacks emanating from data centers and hosting providers. This Working Group will examine and make recommendations to the Council regarding network level best practices and other measures to mitigate the effects of DDoS attacks from large data centers and hosting sites. These recommendations should include technical and operational methods and procedures to facilitate stakeholder implementation of the recommended solution(s).

**Duration:**

1.

#### **Working Group 6 – Long-Term Core Internet Protocol Improvements**

**Chair – Bill Check, CTO NCTA**

**FCC Liaison – Kurian Jacob**

**Description:** The protocols used to govern the operation of the Internet Domain Name System (DNS) are vulnerable to spoofing attacks that can lead to misdirected web requests and consequent on-line fraud. At present, ISPs have been implementing a variety of best practices to work around these weaknesses. One method that has been promoted to address on a long-term basis is adoption of the Domain Name System Security Extensions (DNSSEC), but DNSSEC remains relatively early in deployment and a number of important technical and operational issues remain open concerning its widespread implementation.

This Working Group will identify and plan for long-term remedies to DNS vulnerabilities, including:

1. Identify unintended consequences of DNSSEC deployment and ways to mitigate these consequences.
2. Alternatives to DNSSEC that accomplish its long-term goals while minimizing undesirable consequences.
3. Methods to achieve long-term remediation of the DNS infrastructure, regardless of the solution(s) recommended.
4. Practical implementation plans to better secure the Domain Name System infrastructure, including a path to DNSSEC deployment by ISPs if that is recommended.

The protocols used to govern the operation of the Internet's crucial inter-domain routing system are vulnerable to spoofing attacks that can result in erroneous traffic flows. In the worst case, these misdirected flows intentionally result in the extrusion of massive amounts of data onto unauthorized networks. At present, ISPs have been implementing a variety of best practices to work around these weaknesses. One method that has been identified to address these vulnerabilities is wide application of the BGPSEC security extensions to today's inter-domain routing protocol, but BGPSEC remains a relatively immature standard and a number of important technical and operational issues remain open concerning its widespread implementation.

This Working Group will identify and plan for long-term remedies to inter-domain routing vulnerabilities, including:

1. Identify unintended consequences of BGPSEC deployment and ways to mitigate these consequences.
2. Alternatives to BGPSEC that accomplish its long-term goals while minimizing undesirable consequences.
3. Methods to achieve long-term remediation of the inter-domain routing infrastructure, regardless of the solution(s) recommended.
4. Practical implementation plans to better secure the inter-domain routing infrastructure, including a path to BGPSEC deployment by ISPs if that is recommended.

**Duration:**

- 1.

**Working Group 7 – Legacy Best Practice Updates**

**Chair – Kyle Malady, SVP Network Resiliency, Verizon  
FCC Liaison – Jerome Stanshine**

**Description:** The majority of the best practices recommended by CSRIC address the reliability and resiliency of legacy communications networks, including 9-1-1 networks and services. CSRIC III took a fresh look at the 9-1-1 best practices, but the other legacy best practices have not been examined since CSRIC II. This Working Group will review the legacy best practices to identify where additional practices may be necessary given changes in technology, practices, or observed reliability trends. The Working Group will then recommend changes to the existing set of best practices to address the topics revealed by the foregoing analysis. Finally, the Working Group will consider revisions to best practices proposed by the Alliance for Telecommunications Industry Solutions and recommend how to incorporate these changes into the wider body of best practices.

**Duration:**

- 1.

**Working Group 8 - Submarine Cable Landing Sites Working Group**

**Chair – Kent Bressie, North American Submarine Cable Association  
FCC Liaison – Michael Connelly**

**DESCRIPTION:** As demonstrated by recent events in other parts of the world, the clustering in close geographic proximity of cable landing station facilities and associated submarine cables increases the risk that a single external event – whether snagged fishing gear, a dragged vessel anchor, an earthquake, or a terrorist attack – could damage multiple submarine cables and severely disrupt U.S. connectivity. Such disruptions would harm U.S. economic and security interests, as submarine cables provide almost all of U.S. international connectivity and significant domestic connectivity for certain U.S. states and territories. Industry has focused largely on geographic diversity and mesh networking as means of promoting network resilience. 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 best practices and recommendations on the appropriate separation distance between existing or planned undersea cables and other objects on the seabed floor that could adversely impact those cables and cause communications disruption. 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. Duration.

**Duration:**

1.

**Working Group 9 – Infrastructure Sharing During Emergencies**

**Chair – Jay Naillon – T-Mobile**  
**FCC Liaison – Eric Panketh**

**Description:** Natural disasters and other hazards can result in the destruction of vital communications assets, leading to disruptions to communications at times when users need them most. In recent years communications providers have explored various methods of sharing infrastructure, such as back-up power assets and spectrum, to compensate for the temporary loss of assets. This working group will examine these options and recommend a set of best practices that service providers could use to more rapidly apply infrastructure sharing methods to sustain communications in future emergencies.

**Duration:**

1.

**Working Group 10 – CPE Powering**

**Chair - Tim Walden – CenturyLink**  
**Co-Chair - Brian Allen – Time Warner Cable**  
**FCC Liaison – John Healy**

**Description:** With the rapid proliferation of VoIP technologies as substitutes for legacy telecommunications services, end-users are now utilizing a service that lacks the lifeline they were once accustomed to. Instead of being powered from the resilient back-up power infrastructure in the serving central office, the user’s home device is powered by a local battery when line power is lost, as often happens during emergencies. Different communications providers have different policies as it relates to powering these devices. This Working Group will recommend best practices for providing back-up power to VoIP customer premises equipment, including best practices for consumer notification.

**Duration:**

1.