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 methods 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.

Duration: June 2014

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.

Duration: September 2014

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: June 2014

Working Group 2 – Wireless Emergency Alerts

Co-Chairs – Brian Josef, CTIA
Co-Chairs – John Madden, NEMA
FCC Liaisons – Aaron Garza, 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.

Furthermore, the 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 how WEA message data can be protected on cellular handsets. In this regard, the Working Group shall take into consideration new and evolving technologies that may improve the network's resilience to cyber threats. The Working Group will also address such other EAS-related issues as assigned to CSRIC by the FCC.

Duration:

1. Report on the issues to be examined by the Working Group.

   September 2013

2. Recommendations to the Commission on WEA testing, including any suggested changes to FCC rules.

   June 2014

3. Recommendations to the Commission on geographic targeting, message content and character limitation.

   December 2014

4. Recommendations to the Commission on WEA security actions and best practices.

   December 2014

5. Recommendations to the Commission on other potential types of WEA alerts such as audio streaming, video streaming and multimedia

   TBD

6. Recommendations to the Commission on alerts to people with disabilities

TBD

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, that the Commission should take to improve the process by which state EAS plans are developed and submitted to the Commission. Such review and recommendations shall include an examination of how the selection and administration of State Emergency Communications Councils (SECCs) can be improved, and how the SECCS may develop and submit state EAS plans for Commission review in manner that optimizes the efficiency and effectiveness of the EAS and imposes minimal burdens on stakeholders. In this regard, the Working Group shall take into consideration the transition of the EAS to the Common Alerting Protocol, and the extent to which state EAS plan filings can be made electronically. 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:

1. Recommend any actions, including best practices, that the Commission should take to improve the process by which state EAS plans are developed and submitted to the Commission. Such review and recommendations shall include an examination of how the selection and administration of State Emergency Communications Councils (SECCs) can be improved, and how the SECCS may develop and submit state EAS plans for Commission review in manner that optimizes the efficiency and effectiveness of the EAS in a manner that imposes minimal burdens on stakeholders.

   March 2014

2. Recommend any actions, including best practices; the Commission should facilitate to promote the security of the EAS.

   Recommended Best Practices

   June 2014

3. Develop and provide recommendations on how the Commission can promote and facilitate both awareness and adoption of the "best practices" guidelines contained in the CSRIC WG3 EAS Security Subcommittee Initial Report (May 2014) (*available at* http://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG-3_Initial-Report_061814.pdf). Particular focus should be placed on awareness and adoption by EAS Participants and, in particular, the smaller sized entities least likely to be aware of such guidelines, unsure of which guidelines would be applicable to their operational situations, uncertain as to how to implement those that do apply. Recommendations should also provide guidance to help such entities to help overcome the obstacles that similarly situated EAS participants face.

   March 2015

Working Group 4 – Cybersecurity Best Practices

Co-Chair – Robert Mayer, USTelecom
Co-Chair – Brian Allen, Time Warner Cable
FCC Liaison – Vern Mosley

Description: In order to provide for confidence in the resilience and reliability of the core public communications functions in the face of cyber threats, Working Group 4 will develop voluntary mechanisms to provide macro-level assurance to the FCC and the public that communications providers are taking the necessary corporate and operational measures to manage cybersecurity risks across the enterprise. The macro-level assurance will demonstrate how communications providers are reducing cybersecurity risks through the application of the NIST Cybersecurity Framework, or an equivalent construct. These assurances: (1) can be tailored by individual companies to suit their unique needs, characteristics, and risks (i.e., not one-size-fits-all), (2) are based on meaningful indicators of successful (and unsuccessful) cyber risk management (i.e., outcome-based indicators as opposed to process metrics), and (3) allow for meaningful assessments both internally (e.g., CSO and senior corporate management) and externally (e.g., business partners).

Duration:

1. Recommend voluntary mechanisms to provide macro-level assurance that communications providers (i.e., broadcast, cable, satellite, wireless, and wireline) are taking the necessary corporate and operational measures to manage cybersecurity risks across their enterprise.

   March 2015

Working Group 5 – Remediation of Server-Based DDoS Attacks

Co-Chair – Pete Fonash, 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. Recommend measures communications providers can take to mitigate the incidence and impact of DDoS attacks from data centers and hosting providers, particularly those targeting the information systems of critical sectors.

   Draft Recommendations: June 2014

   Final Recommendations: September 2014

Working Group 6 – Long-Term Core Internet Protocol Improvements

Chair – William Check, NCTA
FCC Liaison – Kurian Jacob

DNS Subgroup – 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. Open DNS Resolvers have been and continue to be a prime target for malicious actors to use to exploit one of the vulnerabilities of DNS and will be used as a case study for this group.

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

- Identify unintended consequences of Open DNS Resolvers and ways to mitigate these consequences.
- Identify best practices for use by the Internet ecosystem (ISPs, ASPs, and CPE vendors) to mitigating issues related to DNS Open Resolvers.
- Methods to achieve long-term remediation of the DNS infrastructure with regard to Open DNS Resolvers, regardless of the solution(s) recommended.
- Recommended implementation steps to mitigate the unintended consequences of Open DNS Resolvers.

Inter-Domain Routing Subgroup – The protocols used to govern the operation of the Internet's crucial inter-domain routing system are vulnerable to attacks that can cause erroneous traffic flows and traffic disruptions. In the worst case, these misdirected flows can result in the

extrusion of massive amounts of data onto unauthorized networks. At present, ISPs have been implementing a variety of best practices to help address these weaknesses. Some extensions (e.g., RPKI, BGPSEC) to today's inter-domain routing protocol have been proposed and are under development; however these extensions and their implementations are still not mature and a number of important technical issues remain open concerning their widespread deployment.

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

- Review of recent Internet route hijacking incidents and review of CSRIC III recommendations to determine if updates are needed.
- Analyze and recommend metrics and measurements related to routing anomalies and attacks.
- Describe practical steps for deployment of protocol extensions (e.g., RPKI) and possible benefits for incremental deployment.
- Develop metrics and measurements to detect reachability issues related to deployment of RPKI or other protocol extensions.

Duration

1. Recommend three categories of best practices or standards (e.g., from CSRIC III Working Group 4 or IETF) for which a detailed implementation plan will be developed by the end of CSRIC IV. The standards could include, for example, BGPSEC or DNSSEC.

   December, 2013

2. Provide interim reports from the DNS subgroup and the inter-domain routing subgroup.

   March, 2014

3. Final reports from the DNS and inter-domain routing subgroups.

   September, 2014

Working Group 7 – Legacy Best Practice Updates

Chair – Kyle Malady, 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. Recommend revisions to legacy CSRIC best practices.

   September 2014

2. Recommend revisions to the prioritizations voted out by CSRIC II based on the recommendations of Working Group 6.

   March 2015

Working Group 8 - Submarine Cable Landing Sites Working Group

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

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:

1. Recommend spatial requirements for undersea cable installation and maintenance.

   September 2014

2. Recommendations for enhancing coordination between and among federal, state, and local agencies without increasing regulatory burdens

   December 2014

3. Recommendations for promoting geographic diversity of routes and landings.

   March 2015

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 and assets, such as back-up power assets and in-market roaming agreements, 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. Recommend for short-term and long-term focus areas.
   Recommend Best Practices and Guidelines for Roaming During Disasters

   June 2014

2. Back-Up Power recommendations

   December 2014

3. Transport recommendations

   December 2014

Working Group 10 – CPE Powering

Chair - Tim Walden, CenturyLink

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. Recommend consumer outreach and communications strategies for making users aware of back-up power features in their home adapter.

   June 2014

2. Recommend best practices for powering consumer devices during commercial power failure.

   September 2014

3. Recommend a continuity plan to ensure that consumer devices remain powered for an acceptable interval in extended disaster scenarios where commercial power is lost.

   December 2014