Updated November 15, 2012

CSRIC III Working Group Descriptions and Leadership

Steering Committee Chair: Stacy Hartman, Director, Federal Public Policy, CenturyLink

Policy

Working Group 1 – NG 9-1-1
Co-Chair – Brian Fontes, NENA
Co-Chair – Laurie Flaherty, NHTSA
FCC Liaison – Patrick Donovan

Description: The Working Group shall recommend additional standards work needed to enable Next Generation 911(NG911) network architecture, particularly those related to the National Emergency Number Association's (NENA's) i3 standard, and related standards needed from other organizations such as Internet Engineering Task Force (IETF), 3rd Generation Partnership Project (3GPP), and Alliance for Telecommunications Industry Solutions (ATIS). The Working Group shall identify gaps in NG911 network architecture standards and label them.

Supplementary Work Description:

1. The Working Group will complete a prioritization of the standards gaps identified in Table 2-4 of of Working Group 1's December 2011 Report. The FCC requests that the prioritization explain which gaps are the most essential to have closed.

    a. Although the alignment of IP Multimedia Subsystem (IMS) with i3 is expected to be completed relatively soon, the FCC requests that the Working Group include the misalignment as a gap until the alignment is finalized.
    b. Working Group 1's December 2011 Report noted that "NENA 77-501 v1 is the initial version of the transition plan to NG911 but there are still gaps remaining for some originating access network types." Working Group 1 will clarify the "access network types" that the report was referring to and whether there is there a problem with the Wireline PSTN and/or Wireless networks. As well, the Working Group will identify how broad or narrow these "access network types" are.
    c. In Section 2.3.7 of Working Group 1's December 2011 Report, the column that included "Identified Gaps" for the Legacy Selective Router Gateway (LSRG) was not complete. The Working Group is tasked with completing this column.

2. The Working Group will prepare a list of interface requirements that will permit an initial version of NG911 to be deployed.

    a. The items in the list should be expressed as results or outcomes, rather than processes or activities. More specifically, the report should provide specific information about the NG911 features and specific protocol interfaces that a

PSAP must implement to receive NG911 calls or text (if text is to be part of Release 1).

b. The list does not need to be overly inclusive. For example, the list does not need to include a complete list of every data, GIS, and logging feature that is internal to the PSAP. The list also does not need to include transition elements, such as the LSRG.

Duration:

1. NG911 Standards- December 8, 2011
2. Prioritization of Standards Gaps- March 22, 2012
3. List of Interface Requirements- June 6, 2012

Working Group 2 – Next Generation Alerting
Co-Chair – Scott Tollefsen, Critical Alert Systems, LLC
Co-Chair – Damon Penn, FEMA
FCC Liaison – Gregory Cooke

Description: The Working Group shall explore all aspects of next generation alerting and develop recommendations for CSRIC's consideration regarding actions the Federal Communications Commission (FCC) should take to promote deployment of next generation alerting systems. The Working Group shall review alerting architectures, such as those used for the Integrated Public Alert and Warning System (IPAWS),[1] the Personal Localized Alerting Network (PLAN), and the distributed architecture presented by the Internet Engineering Task Force (IETF) Authority to the Citizen Alert (ATOCA) Working Group.[2] The Working Group shall consider the manner in which these architectures, and any others under development, may interoperate and interconnect to assure effective delivery of alerts. In addition, the Working Group shall examine different communications distribution platforms, (*e.g.*, Internet, Satellite, Digital Television (DTV) Datacast, etc.) for alert delivery and discuss how the various architectures exploit these distribution platforms. The Working Group shall also explore what alert delivery media (*e.g.*, video, audio, text, graphics, etc.) can be used for the most effective delivery of next generation alerts and develop recommendations regarding how the receiving platforms (e.g., mobile phone and other wireless devices, broadcast, cable, satellite, laptops, tablets etc.) may best present the transmitted alerts to users.

In addition, the Working Group shall develop recommendations regarding the technical and operational criteria under which next generation alerting participants can utilize the Internet and other broadband-based architectures. The operational criteria shall include the relationships among different entities, including, local, tribal, state and federal governments in generating and distributing alerts. The technical requirements shall include consideration of the Common Alerting Protocol and any other protocols for generating, formatting, and distributing alerts, as well as any security requirements (including any trust models) to mitigate potential threats and attacks on the alerting systems.

[1] http://www.fema.gov/emergency/ipaws/
[2] https://datatracker.ietf.org/meeting/79/materials.html#wg-atoca

Finally, the Working Group will explore and develop recommendations regarding the role of social media in next generation alerting systems, including how governments may integrate social media into their own alerting systems.

Duration: March 6, 2013

Working Group 3 – E9-1-1 Location Accuracy
Co-Chair – Steve Wisely, APCO
Co-Chair – Richard Craig, Verizon Wireless
FCC Liaison – Patrick Donovan

Description: The Working Group shall address questions referred to CSRIC in PS Docket No. 07-114, "Wireless E911 Location Accuracy Requirements." In particular:

Outdoor Location Accuracy
The Working Group shall develop approaches to outdoor location accuracy testing criteria, procedures, and timeframes that are reasonable and cost-effective, considering alternatives to current FCC Office of Engineering and Technology OET Bulletin 71. It shall also develop recommendations concerning the feasibility of flexible testing criteria and methodologies, and gather detailed cost data relating to particular testing methodologies from stakeholders to substantiate concerns about potential expense of periodic testing.

Indoor Location Accuracy
It has been widely recognized that indoor location accuracy testing poses unique challenges for carriers. For example, indoor environments are more diverse than outdoor environments. In addition, most homes and buildings are privately owned, thus, access to indoor environments for testing can be difficult.
It is frequently noted that existing location technologies do not perform effectively in all environments. Thus, issues of yield, not just accuracy, are relevant. For example, Assisted Global Positioning System (A-GPS) may not work deep inside a steel-and-concrete building, or even in a suburban residential basement, but may work in wood frame construction, or near office windows.

The FCC's Public Safety and Homeland Security Bureau (Bureau) has not been presented with reliable statistics on the percentage of 911 calls that are made indoors, nor has the Bureau been presented with reliable statistics on the number of emergency calls that are placed within different types of indoor structures (e.g., the fraction of calls placed from concrete-and-steel vs. wood frame construction), or the displacement within the building (e.g., near windows vs. deep inside the structure).

Today, a carrier is likely to locate an indoor 911 caller by using a combination of A-GPS and network triangulation. In the near future, additional location technologies may be able to provide indoor location determination for 911 callers, such as Wi-Fi positioning and femtocells.
The Working Group will address the following questions:

- Do you agree with the basic premises of the paragraphs above?

- Define the scope of "indoors." Should it include non-residential structures, such as airports, stadiums, malls, and warehouses?

- Is it necessary to establish the ratio of indoor vs. outdoor 911 calls? If so, how should such a ratio be determined? Should indoor testing be a separate parameter that is independent of outdoor measurements? In this scenario, a Commercial Mobile Radio System (CMRS) provider would have to independently meet both the indoor and outdoor criteria.

- Should indoor locations be sampled in a statistical manner within each county or PSAP coverage area? This approach would be based on the Commission's decision in its 2010 Location Accuracy Second Report and Order. Should the Commission establish a set of typical indoor scenarios and test each handset model, or class, in one or more model environments? This approach may be appropriate if performance is likely to depend on handset characteristics, such as the GPS chipset, or antenna configuration. Are there other test methodologies that should be considered?

- For CMRS providers that primarily rely on A-GPS, would measuring the effective sensitivity (e.g., measured in dBm) of the GPS receiver, using a suitable bench setup, be sufficient to estimate the achievable indoor location yield and accuracy? Are there other factors that should be taken into account?

- If a GPS sensitivity measurement were used to predict indoor yield and accuracy, how would the receiver sensitivity be translated into these parameters, given the difficulty of statistically estimating the GPS attenuation characteristics across indoor locations? Should such a translation be avoided?

- Some networks use hybrid location technologies, i.e., combine A-GPS with triangulation. As long as an indoor location allows wireless carriers to provide service, would the performance of the triangulation technique differ substantially indoors, e.g., due to differences in multipath characteristics for indoor locations, or strong dependence of the technology on signal strength?

- When testing for location accuracy and yield, should the ability of a carrier to use distributed antenna systems, WiFi, or femtocells be considered? If not, should these techniques be considered at a later date, when they are more likely to be used for 911 purposes? If such techniques should be considered now or at a later date, how should they be considered?

Leveraging Commercial Location-Based Services

The Working Group shall explore and make recommendations on methodologies for leveraging commercial location-based services for 9-1-1 location determination and provide recommendations on the feasibility or appropriateness for the Commission to adopt operational

benchmarks that will allow consumers to evaluate carriers' ability to provide accurate location information.

Duration:

1. Report on Outdoor Testing Criteria- March 22, 2012
2. Report on Indoor Testing- June 6, 2012
3. Report on Indoor Testing Test Bed – September 12, 2012
4. Report on commercial location-based services- March 6, 2013

Network Security

Working Group 4 – Network Security Best Practices

Chair – Rod Rasmussen, Internet Identity
FCC Liaison – Kurian Jacob

Description: This Working Group will examine and make recommendations to the Council regarding best practices to secure the Domain Name System (DNS) and routing system of the Internet during the period leading up to the successful global implementation of the Domain Name System Security Extensions (DNSSEC) and Secure BGP (Border Gateway Protocol) extensions.

DNS is the directory system that associates a domain name with an IP (Internet Protocol) address. In order to achieve this translation, the DNS infrastructure makes hierarchical inquiries to servers that contain this global directory. As DNS inquiries are made, their IP packets rely on routing protocols to reach their correct destination. BGP is the protocol utilized to identify the best available paths for packets to take between points on the Internet at any given moment. This foundational system was built upon a distributed unauthenticated trust model which was sufficient for the early period of the Internet.

These foundational systems are vulnerable to compromise through operator procedural mistakes as well as through malicious attacks that can suspend a domain name or IP address's availability, or compromise their information and integrity. While there are formal initiatives under way within the IETF which has been chartered to develop Internet technical standards and protocols that will improve this situation significantly, global adoption and implementation will take some time.

This Working Group will examine vulnerabilities within these areas and recommend best practices to better secure these critical functions of the Internet during the interval of time preceding deployment of more robust, secure protocol extensions.

Duration:

1. DNS Security Best Practices- September 12, 2012
2. Routing Security Best Practices- March 6, 2013

Working Group 5 – DNSSEC Implementation Practices for ISPs

Chair – Steve Crocker, Shinkuro and ICANN
FCC Liaison – Nnake Nweke

Description: The Domain Name System Security Extensions (DNSSEC) are widely recognized as the best hope for improving the long-term security of the Internet's critical domain name system. Standards for DNSSEC are now mature and implementation has begun in the government as well as the enterprise sector.

This Working Group shall recommend the best practices for deploying and managing the Domain Name System Security Extensions (DNSSEC) by Internet service providers (ISPs). In addition, the Working Group shall recommend proper metrics and measurements that allow for evaluation of the effectiveness of DNSSEC deployment by ISPs. In addition to any other metrics, the Working Group shall address the following: availability of a zone, verification of received data, and validation of verified data. Finally, the Working Group shall recommend ways for the ISP community to demonstrate their intent to deploy DNSSEC, possibly by way of a voluntary opt-in framework.

Duration:

1. DNSSEC Implementation Practices for ISPs- March 22, 2012
2. DNS Security Performance Metrics & ISP Best Practices for Implementing Validation in Their Recursive Resolvers- December 5, 2012
3. Status of DNS Security Performance Metrics- March 6, 2013

Working Group 6 – Secure BGP Deployment

Co-Chair – Andy Ogielski, Renesys
Co-Chair – Jennifer Rexford, Princeton University
FCC Liaison – Randy Bachman

Description: The Border Gateway Protocol (BGP) controls inter-domain routing on the globally routable Internet. BGP relies on trust among operators of gateway routers to ensure the integrity of the Internet routing infrastructure. Over the years, this trust has been compromised on a number of occasions, revealing fundamental weaknesses to this critical Internet utility.

This Working Group will recommend the framework for an industry agreement regarding the adoption of secure routing procedures and protocols based on existing work in industry and research.[3] The framework will include specific technical procedures and protocols. The framework will be proposed in a way suitable for opt-in by large Internet Service Providers (ISPs) in order to create incentives for a wider scale ISP deployment of secure BGP protocols and practices in a market-driven, cost-effective manner.

Duration:

[3] See, for example, "Let the Market Drive Deployment: A Strategy for Transitioning to BGP Security," Gill, Schapira, Goldberg.

1. Secure Routing Implementation Practices – March 22, 2012
2. Secure Routing Performance Metrics– September 12, 2012
3. Status of Secure Routing Performance Metrics– March 6, 2013

Working Group 7 – Botnet Remediation

Co-Chair – Michael O'Reirdan, Messaging Anti-Abuse Working Group
Co-Chair – Peter Fonash, Department of Homeland Security
FCC Liaison – Vern Mosley
FCC Liaison – Kurian Jacob

Description: This Working Group will review the efforts undertaken within the international community, such as the Australian Internet Industry Code of Practice, and among domestic stakeholder groups, such as IETF and the Messaging Anti-Abuse Working Group, for applicability to U.S. ISPs. Building on the work of CSRIC II Working Group 8 ISP Network Protection Practices, the Botnet Remediation Working Group shall propose a set of agreed-upon voluntary practices that would constitute the framework for an opt-in implementation model for ISPs. The Working Group will propose a method for ISPs to express their intent to op-into the framework proposed by the Working Group.

The Working Group will also identify potential ISP implementation obstacles to the newly drafted Botnet Remediation business practices and identify steps the FCC can take that may help overcome these obstacles.

Finally, the Working Group shall identify performance metrics to evaluate the effectiveness of the ISP Botnet Remediation Business Practices at curbing the spread of botnet infections.

Duration:

1. Code of Conduct- March 22, 2012
2. Barrier to Code Participation (Rather than: Incentives for ISPs to Opt-In) & Botnet Remediation Performance Metrics - March 6, 2013

Best Practice Updates

Working Group 8 – E9-1-1 Best Practices
Chair - Robin Howard, Verizon
FCC Liaison – Jerome Stanshine

Description: 9-1-1 service is a vital part of the nation's emergency response and disaster preparedness system and 9-1-1 service reliability is vital to public safety and consumer wellbeing. As such, during CSRIC II, and before that NRIC, a substantial body of voluntary best practices was developed to promote 9-1-1 reliability. 9-1-1 best practices are vital to maintaining a dependable and efficient 9-1-1 infrastructure.

This Working Group will review the existing CSRIC/NRIC 9-1-1 best practices and recommend ways to improve them, accounting for the passage of time, technology changes, operational

factors, and any identified gaps. As part of this effort, the Working Group will also provide recommendations regarding the creation of two new non-industry best practice categories: (i) Public Safety Answering Point (PSAP) and (ii) 9-1-1 Consumer. As well, the Working Group will provide recommendations regarding how to better engage PSAPs in the best practice process.

Finally, this Working Group is tasked with modifying and/or developing new best practices that will support communication providers in preparing for natural or manmade disasters. These best practices will ensure that communication providers are able to restore service quickly in the aftermath of a disaster.

Duration:

1. Disaster Best Practices– June 6, 2012
2. 911 Best Practices– December 5, 2012

Working Group 9 – Alerting Issues Associated With CAP Migration
Co-Chair - Edward Czarnecki, Monroe Electronics
Co-Chair - Chris Homer, DIRECTV
FCC Liaison – Eric Ehrenreich

Description: As the Emergency Alert System (EAS) community migrates from legacy alerting platforms to Common Alerting Protocol (CAP)-based platforms, there is a need for common deployment plans and best practices to help assist with the transition. The Working Group will make recommendations to CSRIC for EAS participants intended to facilitate their CAP migration processes.

Duration:

1. Best Practices to Facilitate CAP Implementation- March 22, 2012
2. CAP implementation at the State and Local Level– June 6, 2012
3. Best practices for CAP Logging and Sign Off- September 12, 2012
4. Implementation Report– March 6, 2013

Working Group 10 – 9-1-1 Prioritization
Co-Chair – Thera Bradshaw, TKC Consulting
Co-Chair – Jeanna Green, Sprint
FCC Liaison – Jerome Stanshine

Description: The working group shall explore ways to ensure that 9-1-1 is available when emergencies or disasters cause a surge in mobile network use. The work will include considerations of how 9-1-1 traffic might be prioritized in such situations. It also includes related operational issues, including ways for PSAPs to address operational issues.

The WG may consider ways to reduce traffic load during emergencies, such as encouragement of use of 911 text as a lower throughput alternative to 911 voice. If the WG pursues arrangements that give 911 calls higher priority than most consumer wireless calls, the WG may consider how to coordinate 911 priority with other priority calling arrangements, including Wireless Priority

Service (WPS), and other arrangements that may provide priority for calls for emergency and first responders. The WG will address implementations in 4G and earlier generation wireless networks; and will consider both E911 and NG911 implementations

Duration: March 6, 2013

Working Group 11 – Consensus Cybersecurity Controls
Co-Chair – Alan Paller, SANS Institute
Co-Chair – Marcus Sachs, Verizon
FCC Liaison – Jeff Goldthorp

Description: This Working Group will examine and make recommendations to the Council regarding technical cybersecurity controls that can provide the most effective possible mitigation of known cyber risks to the business systems and networks maintained by communications providers and to the data maintained on and processed by those systems.

In carrying out its work, the working group will evaluate and contrast the "critical cyber security controls" adopted by the National Security Agency, the Department of Homeland Security in the United States, the UK Centre for the Protection of National Infrastructure and the Australian Defence Signals Directorate, with the existing set of CSRIC cybersecurity best practices. The working group will assess the degree to which the consensus lists of critical controls are applicable to the communications industry, identify gaps between the critical controls and the existing CSRIC best practices, and recommend a superset of the most critical controls for application in the communications industry. The Working Group will recommend updates to the best practices list compiled by CSRIC II with a prioritized list of critical cybersecurity controls that are applicable to the communications industry.

Duration:

1. Revised, prioritized list of critical cybersecurity controls - March 6, 2013