

CSRIC Working Group Descriptions

Working Group 1A - Public Safety Consolidation - Best Practices and Recommendations¹

Description: Public safety radio systems and communications/dispatch centers were historically built and operated by single agencies for their own users. Systems were designed to meet unique local requirements, but often led to incompatibility, inefficient use of scarce resources, and higher costs for specialized equipment and procedures with little opportunity to benefit from economies of scale. However, there has been a clear trend over the last 20 years towards public safety system consolidation, with radio networks developed to cover counties, regions, and even states. Similarly, jurisdictions have merged their communications/dispatch centers across agencies and jurisdictions. The result has been greater economies of scale, more efficient use of limited financial and personnel resources, and improved interoperability. The consolidation process poses numerous challenges, however, from operational, governance, funding and technical perspectives. This Working Group will define these challenges and develop recommended best practices for overcoming them for CSRIC's consideration. A key issue is how to assist agencies in the transition from system operator to system user.

Duration: Six months

Working Group 2A – Cyber Security Best Practices

Description: Communications providers and users are under constant assault from a collection of cybercriminals and others with even more malicious intent. While a large body of cyber security best practices was previously created by the Network Reliability and Interoperability Council (NRIC), many years have passed and the state of the art in cyber security has advanced rapidly. This Working Group will take a fresh look at cyber security best practices, including all segments of the communications industry and public safety communities. The work should be informed by the cyber security work that was previously done in NRIC VI and VII.

Duration: Completion of charter with mid-term readout at nine months.

Working Group 2B – MSRC Best Practice Updates

Description: The Media Security and Reliability Council (MSRC) produced a number of best practices to the security and reliability of commercial broadcast, CATV and MVDS systems. These best practices were last reviewed in December 2005, and much has happened in the intervening years. Some of the best practices may be obsolete, some may be in need of improvement, and others may need to be supplemented. This Working Group will analyze the MSRC best practices and recommend improvements to bring them up-to-date for CSRIC's consideration.

Duration: Completion of charter

¹ The initial focus of the work group will be on a transition to consolidated systems that continue to be operated and controlled by public safety entities, but on a larger scale. A future work group may consider the findings of this group in addressing longer term transitions to networks that are owned or operated, at least in part, by non-public safety entities.

CSRIC Working Group Descriptions

Working Group 4A – Best Practices for Reliable 9-1-1 and E9-1-1

Description: Section 101 of the New and Emerging Technologies 911 Improvement Act (codified at 47 U.S.C. § 615a-1(h)) requires the FCC to develop several best practices related to the implementation of 9-1-1 service for IP-enabled voice service providers, commonly known as VoIP Providers. A significant set of this information may already be available.²

Working Group 3A will investigate and evaluate currently available 9-1-1 related VoIP standards and best practices related to Enhanced 9-1-1 (E9-1-1) for completeness and identify any gaps, including challenges related to implementation of such standards by VoIP providers within the E9-1-1 system. The Working Group will evaluate and recommend to CSRIC how to resolve any incomplete work and gaps, identify and recommend what groups should perform that work (including the option of the CSRIC WG doing so), and recommend to CSRIC an appropriate work schedule.

Duration: Three months.

Working Group 4B – Transition to NG9-1-1³

Description: Building on the work of Working Group 4A, investigate and determine what changes or additions in 9-1-1 related VoIP standards and best practices are required for the evolution of IP-based originating service providers to the IP-based Next Generation 9-1-1 system environment, both during the transition from E9-1-1 to NG9-1-1 and as identifiable for the longer term all-IP NG9-1-1 environment. The Work Group will consider technical issues as well as operational and funding challenges for PSAPs in a NG9-1-1 environment. The Working Group will also consider ways that NG9-1-1 architectures and technologies can improve 9-1-1 access for people with disabilities and non-English speaking communities. The Work Group will evaluate and recommend to CSRIC how the changes and additions to standards and best practices should be accomplished, what groups should perform that work (including the option of the CSRIC WG doing so), and an appropriate work schedule.

Duration: Twelve months from the completion of Working Group 4A or completion of charter, whichever comes first.

Working Group 4C – Technical Options for E9-1-1 Location Accuracy

Description: Examine E9-1-1/Public Safety location technologies in use today, identifying current performance and limitations for use in NG Public Safety Applications

Examine emerging E911/Public Safety location technologies and recommend options to CSRIC for improvement of E9-1-1 location accuracy including implementation timelines. These recommendations should include:

² NENA, for example, has created a large body of best practices that appear to satisfy the statute's intent.

³ Assumes same WG will be used for WG3A and WG3B.

CSRIC Working Group Descriptions

- Identify industry standards direction for location and ability to use location for next generation services and applications.
- Identify emerging location technologies, including combining multiple technologies to improve location accuracy
- Identify when such technologies could be available
- Identify security issues and vulnerabilities around future location technologies
- Identify interactions with existing technologies and any backwards compatibility issues
- Identify opportunities to apply next generation location technologies to current networks
- Identify impacts to user equipment, networks, agencies, etc. for deployment of future E911/Public Safety location accuracy technologies
- Identify barriers to deploying these technologies

Duration: Twelve months

Working Group 5A – CAP Introduction

Description: In its May 2007 EAS Second Report and Order (EB Docket No. 04-296), the Commission mandated that all EAS Participants must be capable of receiving a CAP-formatted EAS alert within 180 days of an announcement by the Federal Emergency Management Agency (FEMA) adopting CAP. The Commission noted that the transformation of the EAS brought about by CAP would necessitate revisions to the Commission's Part 11 rules governing the EAS. The Working Group should specifically base their recommendations on the Oasis-published CAP 1.2, and include in their discussion both specific recommendations regarding rule changes and more general comment and analysis regarding the appropriate Part 11 regulatory structure for a CAP-based EAS. The Working Group should also recommend actions the FCC can take to improve EAS access for people with disabilities and non-English speaking communities.

Duration: Six months

Working Group 6 – Best Practice Implementation

Description: This working group will develop options and recommendations for CSRIC's consideration regarding the key best practices for each communications industry segment that should be implemented by communications service providers in order to enhance the security, reliability, operability and resiliency of communications infrastructure. The working group will also develop options and recommendations, for CSRIC's consideration, options and recommendations for methods to measure reliably and accurately the extent to which these key best practices are being implemented. In fulfilling this task, the working group will examine best practices previously recommended by the former Network Reliability & Interoperability Council and the former Media Security & Reliability Council as well as any best practices that may be approved by the CSRIC.

CSRIC Working Group Descriptions

Duration: Completion of charter.

Working Group 7 – Pandemic Planning – Priority Service Requirements

Description: In the event of a major outbreak of infectious disease there will be a tendency for large groups of people to telecommute to avoid clustering in common locations. This migration from enterprise to residence will be difficult to plan for and may lead to congestion in communications networks. The national security and emergency preparedness (NS/EP) community has access to effective priority communications services that enable members to complete emergency calls even during times when networks have sustained considerable damage, and, thereby have limited capacity, and times of extreme congestion. The primary systems are the government emergency telecommunications service (GETS) and wireless priority service (WPS). These systems were designed to operate with circuit switched networks. As the networks evolve toward internet protocol (IP) networks, and the NS/EP community migrates to these networks and services, fewer and fewer members of the NS/EP community will be able to rely on these priority services to complete their essential communications. As a result, it is incumbent that network operators develop NS/EP priority services for the next generation IP-based networks. To help with this development, we are assigning the following tasks to the CSRIC: (1) develop a NGN IP priority service requirements document that specifies the order of magnitude of users, types of services covered (e.g., voice, data, video, others), number of levels of priority, processes for authorizing priority access, performance standards/metrics, and expected costs; and (2) develop a priority services implementation strategy (e.g., which types of service should be rolled out first).

Duration: Twelve months.

Working Group 8 – ISP Network Protection Practices

Description: This Working Group will investigate current practices that ISPs use to protect their networks from harms caused by the *logical* connection of computer equipment, as well as desired practices and associated implementation obstacles.⁴ The work should address techniques for dynamically identifying computer equipment that is engaging in a malicious cyber attack, notifying the user, and remediating the problem. The Working Group will develop proposed recommendations for CSRIC's consideration for best practices and actions the FCC could take that may help overcome implementation obstacles.

Duration: Twelve months.

⁴ As used here "computer equipment" includes a wide variety of personal equipment (*e.g.*, servers, PCs, smart phones, home routers, *etc.*) as well as household devices with embedded IP network connectivity. "logical connection" refers to end-user data communications protocol signaling and transmission. Harms result from the ability to degrade the communications infrastructure through malicious protocol exchanges and information transmission.