

STANDARDIZATION FOR EMERGENCY COMMUNICATIONS

DRAFT WORKSHOP REPORT

Organizer

ANSI Homeland Security Standards Panel (HSSP)

Report publication date

April 2008

More information

www.ansi.org/hssp



ANSI Homeland Security Standards Panel

25 West 43rd Street – Fourth Floor

New York, NY 10036

T: 212.642.4992

F: 212.398.0023

E: mdeane@ansi.org

TABLE OF CONTENTS

Introduction	3
Background for the ANSI-HSSP Workshop	3
Workshop Objectives and Launch	4
Continuation of Workshop Efforts	6
Findings and Recommendations	8
Conclusion.....	32
Annex A – Participation	33
Annex B – Global Standards Collaboration	35
Annex C – Government-to-Government Emergency Communications	36
Annex D - NENA NG9-1-1 Design (with IETF)	37
Annex E – Glossary of Terms and Acronyms.....	38
Annex F – Additional Resources for Government-to-Government Emergency Communications.....	40

Introduction

Effective “*emergency communications*” is an essential component of homeland security, as well as that of preparedness, response, and recovery efforts. However, the term “emergency communications” can often mean different things to different people or organizations. For some, it is simply “tele” communications. For others, it is the “content” of the message or communications, not the media or facilities used to deliver the content. And for others, “emergency communications” only come from a recognized governmental body.

In addition to these definitional issues, emergency communications must cut cross-sector and cross-technology areas to be effective and harmonized, as well as to send an unambiguous, important communication. Truly effective emergency communications also takes into account persons with disabilities and individuals whose primary language is not English.

This report seeks to address these challenges and provide some guidance via standardization for various aspects of emergency communications. The report highlights the primary stakeholders and resources in this subject area, the key challenges and issues that exist, and further areas for exploration in the area of emergency communications, especially those pending further governmental decision making. Material for this report comes from the ANSI Homeland Security Standards Panel (ANSI-HSSP) Workshop meetings held to explore standards and conformity assessment issues regarding emergency communications, from ANSI-HSSP Plenary meetings, and from other sources and events subsequent to the ANSI-HSSP Workshop meetings.

Background for the ANSI-HSSP Workshop

The ANSI Homeland Security Standards Panel ([HSSP](#)) has as its mission to identify existing consensus standards, or if none exists, assist the U.S. Department of Homeland Security (DHS) and those sectors requesting assistance to accelerate development and adoption of consensus standards critical to homeland security. The ANSI-HSSP promotes a positive, cooperative partnership between the public and private sectors in order to meet the needs of the nation in this critical area. To address specific homeland security standards areas, Workshops are convened under the ANSI-HSSP to bring together subject matter experts in that particular security area.

Following the launch of the ANSI-HSSP, the subject of emergency communications was endorsed as one of areas that the Panel would address via a [Workshop](#). Dan Bart, at the time Chief Technology Officer (CTO) and Advisor to the President at the Telecommunications Industry Association (TIA) and private sector ANSI-HSSP Co-Chair, was endorsed by the ANSI-HSSP Steering Committee to serve as the leader for this Workshop effort.

Workshop Objectives and Launch

The Workshop was created with the objectives of identifying existing standards, standards under development, and gap areas in standardization for emergency communications. The Workshop also was tasked with examining the current state or need for accreditation and certification programs to support these standards. An [ANSI-HSSP Workshop website](#) contains the presentations and other documentation from the Workshop meetings that were held.

The first ANSI-HSSP Emergency Communications Workshop meeting was held December 1-2, 2004 at Motorola Headquarters in Schaumburg, IL.¹ Conclusions from the Global Standards Collaboration (GSC) were used as the starting point for focusing the efforts of the Workshop.² Resolution GSC-8/1: Emergency Communications (Ottawa 2003) concluded that emergency communications can be partitioned into concerns covering communications:

- (1) from citizens to authorities and/or organizations providing emergency services,
- (2) between such authorities,
- (3) from such authorities to citizens, and
- (4) amongst affected citizens.

This resolution further added that it is important for GSC Participating Standards Organizations (PSOs), as well as authorities and/or organizations providing emergency services in countries across the world, to continue to collaborate in the development of technical standards, and to share information on emerging technologies and services that can be used for emergency communications.

Following discussion among Workshop participants, it was agreed that the Emergency Communications Workshop should address three of the four “legs” of emergency communications:

¹ See *Annex A* for organizations that were represented.

² See *Annex B* for more information on the GSC.

- **citizen-to-citizen** - An individual communicating an emergency to another individual or private organization via available options (*e.g.*, OnStar-like message, amateur radio, mobile and land-line communications, broadcast and mass media, Internet, email lists, faxes, information services, and word of mouth).
- **citizen-to-government** - An individual communicating an emergency message to appropriate authorities via available options (*e.g.*, E9-1-1/1-1-2 call to a Public Safety Answering Point (PSAP), amateur radio, and mobile communications).
- **government-to-citizen** - Government or authorized officials communicating alerts or details of an emergency to individuals and organizations via available options (*e.g.*, governmental mass media alerts, citizen accessible radio services and common channels, highway alerts, voluntary private-sector alert services [localized and national], e-mail/voice-mail and word of mouth).

The **government-to-government** “leg” was omitted from the Workshop due to it being covered in numerous other venues.³ This leg of emergency communications includes governmental authorities communicating to each other, other agencies, and appropriate National Security/Emergency Preparedness (NS/EP)-designated private industry concerns and coordinators (*i.e.*, using all forms of communications services, private radio (*i.e.*, land mobile radio [LMR]), Commercial Mobile Radio Services, e-mail/messaging alerts, etc.).

During the Workshop meeting, presentations were delivered on each of the three legs of emergency communications to be addressed, followed by breakout sessions to examine each in further detail. The focus of each breakout session was to begin to lay the groundwork for the process of identifying existing standards or work in process (including how to classify/categorize them), as well as how to best identify gap areas where standards still are needed. As with all ANSI-HSSP Workshops, the issue of Conformity Assessment (accreditation and certification) was introduced in each breakout. The Workshop leader instructed each breakout session to also address the issues of reaching non-English speakers and persons with disabilities.

³ See *Annex C* for a listing of entities addressing this leg of emergency communications.

Continuation of Workshop Efforts

Task groups were created at the kick-off Workshop meeting for each of the three legs of emergency communications to further explore these areas from a standards perspective. While this work occurred, there were several initiatives already identified and underway that the Workshop monitored as those findings/recommendations could possibly have an impact on the direction of the Workshop. Of major importance was the work being conducted by the Federal Communications Commission's (FCC) Seventh Network Reliability and Interoperability Council (NRIC VII). Among NRIC VII's objectives and scope of work were to provide recommendations to the FCC and the communications industry that would facilitate the reliability, robustness, security, and interoperability of communications networks including emergency communication networks. Under Focus Group 1 – Enhanced E911, four subcommittees met to study near-term requirements, long-term requirements, network outages and best practices, and PSAP/Emergency Communications Beyond E911.⁴ The follow-up Emergency Communications Workshop meeting was held December 14-15, 2005 at the National Institute of Standards and Technology (NIST) in Gaithersburg, MD. Participants reviewed Resolution [GSC-10/02](#): (Joint) Emergency Communications (Sophia-Antipolis 2005) which was an update to the prior GSC-8 resolution:

Resolves:

1. to establish a continuing area of work on “emergency communications” to further encourage cooperation and the sharing of information among SDOs, ITU, and others working on standardization activities relating to communications in emergency situations, in particular addressing
 - communications from individuals/organizations⁵ to authorities
 - communications between and among authorities
 - communications from authorities to individuals/organizations
 - communications amongst affected individuals/organizations

including, but not limited to, developing standards applicable to existing and future systems for:

- technical means for delivery of early warnings or alerts

⁴ The NRIC VII charter can be found at:
http://www.nric.org/charter_vii/NRICVII_Charter_FINAL_Amended_2004_3_12_04.pdf

⁵ Use of the term “individuals/organizations” is intentionally broad and intended to include citizens, non-citizens and visitors, employer-to-employee emergency communications, as well as employer-to-employer, and also encompasses the unique concerns for persons with disabilities and those individuals who may not be fluent in the language(s) or dialects in use in the locus of the emergency or disaster.

- priority access to emergency call access numbers;
- provision of location information;
- suitable technologies for use in networks dedicated to public protection and disaster relief communications;
- interoperability between public networks and networks dedicated to emergency communications;
- priority access by emergency services personnel to communications services

Resolves:

2. to encourage ongoing cooperation and collaboration among national, regional and international activities that relate to emergency communications, such as Project MESA and to provide forums to collect aggregated government users' needs at the local, state or provincial, or national/international level;
3. to encourage PSOs to support ongoing national activity and cooperation between industry, PSOs, administrations and authorities in the establishment of emergency communications and harmonize terminology used, for example, use of the term "emergency communications" and not "emergency telecommunications" in order to embrace and include the widest range of new systems, services, and technologies and not just "telecommunications";
4. to draw to the attention of PSOs the need to examine the characteristics of providing emergency communications over packet-based networks, including Next-Generation Networks; and
5. to enhance collaborative efforts at the international level to make most efficient use of resources and enable a timely and focused approach in the global deployment of systems and solutions.

The term "citizen" is too narrow, since non-citizens, visitors and others are also use emergency communications. The ANSI-HSSP Workshop agreed to replace the word "citizen" with "individual/organization," in the future, creating:

- Individuals/Organizations-to-Individuals/Organizations (including Employer-to-Employee, and Employer-to-Employer)
- Individuals/Organizations-to-Government
- Government-to-Individuals/Organizations

Prior to continuing the work in each of these areas via breakout sessions, panel sessions at this meeting covered a number of key areas for emergency communications. These included:

- Emergency communications lessons learned from hurricanes Rita, Katrina, and Wilma (both from the perspective of public safety and others involved in providing emergency communications, but also from the recipient of the communications, including issues communicating to persons with disabilities)
- FCC Activities Supporting Homeland Security and Emergency Communications
- NRIC VII Review of PSAPs in 2010
- Congressional Initiatives to Create a National Alert System - S. 1753 the WARN Act
- New Technology Initiatives for Emergency Communications (satellite, secure conferencing and web collaboration).

Findings and Recommendations

This section provides information on the findings from each of the Workshop breakout areas, including areas for further exploration, and recent developments since the conclusion of the Workshop meetings.

Individuals/Organizations-to-Individuals/Organizations (including employer-to-employee, employer-to-employer)

The primary standard⁶ identified as providing guidance for individuals/organizations to individuals/organizations communications during an emergency was [NFPA 1600](#), *Standard on Disaster/Emergency Management and Business Continuity Programs*. This American National Standard was recommended by the Federal 9/11 Commission as the standard for private-sector preparedness, and it has been endorsed/adopted by a number of federal agencies, as well as being referenced in various pieces of federal legislation. Clause 5.9 of the standard addresses “Communication and Warning,” providing guidance on the key issues that need to be addressed and examined in further detail in this area. The Workshop breakout group recommended NFPA 1600 for this category of emergency communications, especially for employer-to-employee and employer-to-employer communications.

During an emergency situation, the traditional methods used for communicating with others are not always available. Such systems may be damaged and out of service or heavily overloaded with traffic. Land-line phones, mobile phones, e-mail, and other devices depend on power availability, something that is often interrupted during an emergency situation. The Workshop breakout group identified amateur radio as an important means of emergency communications when traditional communication means are interrupted. The identification of an amateur radio operator (also called ‘ham’ radio operator) in an individual’s neighborhood or work environment is an important measure to take to be prepared.

The Amateur Radio Emergency Service (ARES) involves FCC-licensed amateur radio volunteers with over 40,000 registered in U.S. These volunteers are trained and experienced operators, ready to respond in emergencies. There is coordination and management at the national, sectional, district and local levels between operators. Simulated Emergency Tests (SETs) are performed of the system and an annual

⁶ As defined by *ISO/IEC Guide 2*, a standard is a “Document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context.”

nationwide exercise finds strengths and weaknesses of ARES and provides public demonstrations to served entities. Further information on amateur radio can be found on the Website for the American Radio Relay League ([ARRL](#)).

Challenges/needs areas identified for amateur radio emergency communications included:

- The terms ‘*amateur*’ and ‘*volunteers*,’ in this context, are misnomers given that these operators are well trained and professional problem solvers (40, 000 in U.S.) ready to assist with emergency communications efforts and fill in the gaps until normalized communications resumes.
- The importance of testing and simulation of systems and situations before you really need it was stressed.
- The usefulness of current RACES (Radio Amateur Civil Emergency Service) guidelines were questioned and the need for industry to consult on this issue.
- Disparate reporting formats for amateur operators; standardization would be beneficial.
- Certification needs for radio volunteers operating outside their “home” jurisdiction (*i.e.*, called to assist at disaster scene).
- The potential of increased international coordination between global amateur radio groups.
- Increased outreach to persons with disabilities (equipment is available and emerging and such activities allow this community to be engaged and play a viable role in emergency response).
- The potential for encryption is emerging [*i.e.*, Health Insurance Portability and Accountability Act (HIPAA) needs] and being addressed by the amateur radio community and eventually the FCC.

Further challenges for community (individual-to-individual) emergency communications planning included:

- Need for emergency dialog and planning by associations, home-owner organizations, local schools and other communities. This includes gathering emergency numbers like cellular phone numbers, emails, pagers, and other means to be notified. Reverse 9-1-1 systems, and systems that can send alerts to defined groups
- Emerging technology can be problematic for 9-1-1 and other emergency service requests (*i.e.*, VoIP) by individuals.
- Emergency communications alternatives if the local 9-1-1 center itself is disrupted.
- People should not rely solely on government or others; they need to be prepared themselves.

- Need for guidelines or best practices for individual/organizational preparedness (included mechanisms for outreach).⁷
- The periodic testing and exercise of such systems.
- Planning for the needs of persons with disabilities and those for whom English is not their native language.

Key resources and information pertaining to this leg of emergency communications include:

- The FCC has [rules](#) that require broadcasters, cable operators, and other multi-channel video programming distributors to make emergency information (*e.g.*, pertaining to storms, school closings, and other emergencies) that they provide to their viewers accessible to persons with hearing and vision disabilities.
- On July 26, 2004, President Bush signed Executive Order No. 13347, which established the *Interagency Coordinating Council on Emergency Preparedness and Individuals with Disabilities (ICC)*. This Executive Order required that disability access be considered in emergency planning and that an annual report be submitted to the President.
 - The Federal Communications Commission has played an active role in the ICC since its inception. The FCC Chairs the Emergency Communications Subcommittee, and is a member of the following subcommittees: Technical Assistance and Outreach; Emergency Preparedness in the Workplace; Emergency Transportation.
 - On July 22, 2005, the ICC adopted an [Annual Report](#) and launched an electronic resource center on emergency preparedness planning for persons with disabilities as well as an emergency preparedness planning template for employers of persons with disabilities.
 - The purpose of the Council is to:
 - Consider, in their emergency preparedness planning, the unique needs of agency employees with disabilities and individuals with disabilities whom the agency serves;
 - Encourage, including through the provision of technical assistance, consideration of the unique needs of employees and individuals with disabilities served by State, local, and tribal governments, and private organizations and individuals in emergency preparedness planning; and
 - Facilitate cooperation among Federal, State, local, and tribal governments and private organizations and individuals in the implementation of emergency preparedness plans as they relate to individuals with disabilities.
- [Ready.gov](#) also provides information for employers and employees in planning their emergency communications needs.
- Gallaudet University conducted a 2-day [Conference: Accessible Emergency Notification and Communication: State of the Science Conference](#), November 2 - 3, 2005, which reviewed the state of the science on the accessibility of emergency communications to people with disabilities. This conference brought together experts in accessibility, mass media, emergency communications, telecommunications, Internet, and government policy to analyze barriers and technological solutions for effective emergency communications with and for people with disabilities. Attendees included

⁷ In response to this identified need, a [Citizen Preparedness](#) webpage was created on the ANSI-HSSP website.

representatives from federal, state, and local government; industry representatives; consumer representatives; and accessibility experts.

- The FCC's Public Safety and Homeland Security Bureau (Bureau) hosted, in conjunction with the U.S. Department of Health and Human Services, a [Health Care Summit on Emergency Communications, Response and Recovery](#) on Thursday, November 1, 2007. The [Summit](#) focused on hospital emergency communications plans and preparedness efforts, including the use of alternative technologies to bolster response capabilities. The Summit also examined the benefits of utilizing broadband networks, to support telemedicine, and other communications infrastructure that will improve information-sharing capabilities and further strengthen the Nation's response to pandemics or bioterrorism-related events.
- On April 16, 2007, one student, senior Seung Hui Cho, murdered 32 and injured 17 students and faculty in two related incidents on the campus of Virginia Polytechnic Institute and State University ("Virginia Tech"). Three days later, Virginia Governor Tim Kaine commissioned a panel of experts to conduct an independent, thorough, and objective review of the tragedy and to make recommendations regarding improvements to the Commonwealth's laws, policies, procedures, systems and institutions, as well as those of other governmental entities and private providers. Each member of the appointed panel had expertise in areas relevant to its work, including Virginia's mental health system, university administration, public safety and security, law enforcement, victim services, emergency medical services, and the justice system. The panel reviewed many areas including "the emergency response by all parties (law enforcement officials, university officials, medical responders and hospital care providers, and the Medical Examiner)."

Included in the [final report](#) were [Guidelines](#) for an emergency communications alerting system which were consistent with ANSI-HSSP Workshop findings to use multiple means of issuing emergency alerts. The recommended successful system in the Virginia Tech report would provide:

- Multi-modal communications;
 - o text messaging (preferably using true Short Message Service [SMS] protocol)
 - o Instant Messaging (IM)
 - o e-mail
 - o Web posting
 - o voice communication to cellular or land line based extensions (including ability to fax)
- Flexibility in "registering" or "subscribing" users;
 - o ability to pre-load based on existing directory data with both APIs and online mechanisms for batch or manual updates
- Robust, but distributed data centers, i.e. more than one location; ability to send alerts even if event impacts vendor's facility
- Robust, but dispersed messaging; concern is with saturation of communications channels (Part of "Lessons Learned" from 9/11 and previous incident in Blacksburg on first day of Fall Semester 2006; "too much, too soon" will quickly overwhelm cellular and land line telephony systems)

- The vendor would have to be flexible in terms of contracting, and willing to collaborate on further developing the product's features to meet specific needs identified by Virginia Tech.

There are now many systems being used and deployed by the private sector as well as by governments to issue alerts for emergency situations. Examples include simple systems being used for traffic alerts and school closings due to weather, to emergency notifications for many threats and hazards, such as:

- [Amber Alerts](#)
- [Emergency email, fax, cell phone alerts](#)
- Local Government alert systems like [Alert DC](#) and the [City of San Diego Reverse 911 System](#):
 - The Alert DC system provides immediate text notification and update information during a major crisis or emergency. This system delivers important emergency alerts, notifications and updates on a range of devices including your:
 - e-mail account [work, home, other]
 - cell phone
 - pager, BlackBerry
 - wireless PDA
 - When an incident or emergency occurs, authorized DC Homeland Security & Emergency Management personnel can rapidly notify you using this community alert system. Alert DC is your personal connection to real-time updates, instructions on where to go, what to do, or what not to do, who to contact and other important information.
 - Alert DC is available to citizens of the District of Columbia as well as individuals traveling to or working in the District.
 - City of San Diego Reverse 911[®] Emergency Notification System: The Emergency Notification System allows the City to rapidly send telephone notifications to all residents and businesses in an affected area in the event of an emergency.
 - An operator using the system can identify the affected neighborhood or region of the city and record a message that describes the situation.
 - The system will automatically call listed and unlisted telephone numbers (including TTY/TDD) within the affected area and deliver the recorded message.
 - If phone lines are busy, the system will attempt to redial those telephone numbers to make contact.
 - If an answering machine picks up the call, the emergency message will be left on the machine.
 - Cellular or Voice over IP (VoIP) phone numbers are not currently in the system database. If you would like to be contacted on your cell or VoIP phone, you must register those phone numbers
- County-Wide-systems like [Arlington County Virginia](#) which includes additional language notifications, Fairfax County's Community Emergency Alert Network ([CEAN](#)), and [San Mateo County](#).
- State-Wide alert systems like in [Louisiana](#) and [Mississippi](#), which became the first state in the nation to develop a secure statewide alert system for emergency responders.

States are also passing laws directed towards the issues of Emergency Communications. For example, in California, on September 29, 2006, Assembly Bill 2393 (AB 2393, Ch. 776, Stats 2006), Levine, "Telecommunications: Emergency Service" was signed into law. It directed the California Public Utilities Commission to investigate the need for performance reliability standards for back-up power systems installed on the property of residential and small commercial customers and telecommunications service providers. It also required the Commission to determine whether standardized notification systems and protocols should be utilized for emergency notification systems. To satisfy these requirements, on April 12, 2007, the Commission opened Rulemaking (R) 07-04-015. The Communications Division (CD) was charged with performing the investigation. CD hired a consultant, SAIC/Telcordia Technologies, Inc., to assist in the investigation. CD's investigation is ongoing.

The legislative concerns embodied in AB 2393 could not have been more timely. Adopted in part in response to concerns raised in the aftermath of Hurricane Katrina, soon after the initiation of this proceeding our nation suffered the violence at Virginia Tech. Most recently California experienced wildfires raging over large portions of Southern California calling into question our preparedness for emergencies, both in terms of our means of emergency communications and back up capabilities for our telecommunications system. California will be holding a workshop on January 9, 2008 that will focus on the performance of the landline and wireless services during the recent firestorm. This workshop will review the ways in which cities, localities and communication carriers responded to the challenges posed by the fires as well as identifying and addressing the communication barriers to best practices for first responders during times of emergency. The goal of the workshop is to identify the next steps toward improving California's ability to maintain network performance in future crises.

AB 2393 requires the Commission to send a report on its investigation to the Legislature before January 1, 2008. The [November 2007 report](#), intended to comply with the legislation, describes progress to date and plans for completion. AB 2393 directed the Commission to:

1. Consider the need for performance reliability standards for backup power systems located on the property of residential and small commercial customers. The Commission is to develop and implement performance reliability standards if the benefits of the standards exceed the costs. (Public Utilities Code § 776);¹
2. Consider, in consultation with the Office of Emergency Services (OES) and the Department of General Services (DGS), whether standardized notification systems and protocols should be utilized to facilitate notification of affected members of the public about local emergencies. (§ 2872); and

3. Consider, in consultation with the OES and the DGS, the need for performance reliability standards for back-up power systems on the telecommunications service provider's premises to enable telecommunications networks to function during an electrical outage. The Commission is to develop and implement performance reliability standards if the benefits of the standards exceed the costs. In addition, the Commission is to determine whether the FCC's National Reliability and Interoperability Committee's Best Practices (Best Practices) for back-up systems have been implemented by telecommunications service providers. (§ 2892.1). The Commission is also to investigate the feasibility of replacing diesel back-up power systems with zero greenhouse gas emission fuel cells.

In support of R. 07-04-015, CD held three technical workshops addressing the subject matter. The first workshop, held on June 5, 2007, addressed back-up power systems on residential and small commercial customers' property. The second workshop, held on June 6, 2007, addressed back-up power systems on service provider premises. The third workshop, held on June 19, 2007, addressed emergency notification systems.

Subsequently, CD issued information requests to augment the information garnered from the above workshops. The informational requests were intended to obtain additional information in each area of investigation, and to provide the opportunity for input from entities who did not attend the workshops.

CD followed-up the informational requests with additional questions because the information received at the workshops and in responses to the initial informational requests was insufficient to perform the necessary analyses. In furtherance of its investigation, CD visited telecom service provider locations. CD is continuing its investigation and plans to perform a statistical analysis of the data received. As required by AB 2393, the Commission will conclude its investigation and issue a final report by June 30, 2008.

The FCC also has a [website](#) to aid with planning for Emergency Communications: Emergency Communications Resources. It includes:

- [Guidelines for Emergency Planning](#). The purpose of the Emergency Planning Guidelines is to provide a framework for emergency preparedness for organizations to use to build their emergency communications plans. The FCC encourages the use of these emergency communications best practices by first responder organizations to improve their emergency communications systems and address unique regulatory or operational requirements which may exist within their organizations. Our guidelines were developed following a thorough review of existing emergency preparedness guidance put forth by several industry groups that developed best practices guidelines.
- [Planning Information Clearinghouse](#). On a continual basis, PSHSB will post examples of emergency communications plans developed and implemented by state government, law enforcement agencies, health care facilities, and first responders. The FCC is sharing this content publicly as a representation of the authors' preparedness plans, which will highlight best

practices in the field of emergency communications.

- [Chief Engineer's Tech Topics](#). As a part of the ongoing Bureau's efforts to disseminate communications information, the Bureau's Chief Engineer regularly provides installments of Tech Topics that should be of interest to the public safety and homeland security communities. The Bureau has the technical and regulatory expertise and resources to assist first responders with information and guidance concerning communication systems, spectrum use, licensing requirements, the value of staff training in the use of communications equipment, and the importance of adopting and refining emergency communications plans, including implementation of backup or alternate communications strategies in cases of prolonged power outages or other disruptions.

In June 2007, the Commission released the *Katrina Panel Order*⁸ directing the Public Safety and Homeland Security Bureau (PSHSB) to implement several of the recommendations made by the Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks (Katrina Panel). Among other things, the Commission adopted a rule requiring some communications providers to have emergency/backup power. The backup power rule adopted specifically states:

- Local exchange carriers (LECs), including incumbent LECs (ILECs) and competitive LECs (CLECs), and commercial mobile radio service (CMRS) providers must have an emergency backup power source for all assets that are normally powered from local AC commercial power, including those inside central offices, cell sites, remote switches and digital loop carrier system remote terminals. LECs and CMRS providers should maintain emergency backup power for a minimum of 24 hours for assets inside central offices and eight hours for cell sites, remote switches and digital loop carrier system remote terminals that are normally powered from local AC commercial power. LECs that meet the definition of a Class B company as set forth in Section 32.11(b)(2) of the Commission's rules and non-nationwide CMRS providers with no more than 500,000 subscribers are exempt from this rule.

In its [Order on Reconsideration](#) released October 4, 2007, the FCC granted in part and denied in part the Petitions for Reconsideration that were filed. The FCC modified Section 12.2 to address several meritorious issues raised in the Petitions. The FCC advised this modification will facilitate carrier compliance and reduce the burden on LECs and CMRS providers, while continuing to further important homeland security and public safety goals. The FCC noted in footnote 25:

See Katrina Panel Report at i (“lack of power and/or fuel” was one of the “three main problems that caused the majority of communications network interruptions”); *id.* at 5-6 (“[T]he duration of power outages far outlasted most generator fuel reserves, leading to the failure of otherwise functional infrastructure.”); *id.* at 9 (“In general, cellular/PCS base stations were not destroyed by Katrina,

⁸ *Katrina Panel Order*, 22 FCC Rcd 10541 (2007).

although some antennas required adjustment after the storm. Rather, the majority of the adverse effects and outages encountered by wireless providers were due to a lack of commercial power or a lack of transport connectivity to the wireless switch”); *id.* at 14 (“While the communications industry has generally been diligent in deploying backup batteries and generators and ensuring that these systems have one to two days of fuel or charge, not all locations had them installed. . . . Where generators were installed and operational, the fuel was generally exhausted prior to restoration of power.”); *id.* at 17 (“Backup generators and batteries were not present at all facilities. Where they were deployed, most provided only enough power to operate particular communications facilities for 24-48 hours – generally a sufficient period of time to permit the restoration of commercial power in most situations, but not enough for a catastrophe like Hurricane Katrina.”).

The amended Rule now reads:

1. Section 12.2 is amended to read as follows:

§ 12.2 Backup Power.

(a) Except to the extent set forth in Section 12.2(b) and Section 12.2(c)(4) of the Commission’s rules, local exchange carriers, including incumbent local exchange carriers and competitive local exchange carriers (collectively, LECs), and commercial mobile radio service (CMRS) providers, as defined in Section 20.9 of the Commission’s rules, must have an emergency backup power source (*e.g.*, batteries, generators, fuel cells) for all assets necessary to maintain communications that are normally powered from local commercial power, including those assets located inside central offices, cell sites, remote switches and digital loop carrier system remote terminals. LECs and CMRS providers must maintain emergency backup power for a minimum of twenty-four hours for assets that are normally powered from local commercial power and located inside central offices, and eight hours for assets that are normally powered from local commercial power and at other locations, including cell sites, remote switches and digital loop carrier system remote terminals. Power sources satisfy this requirement if they were originally designed to provide the minimum backup power capacity level required herein and the provider has implemented reasonable methods and procedures to ensure that the power sources are regularly checked and replaced when they deteriorate. LECs that meet the definition of a Class B company as set forth in Section 32.11(b)(2) of the Commission’s rules and non-nationwide CMRS providers with no more than 500,000 subscribers are exempt from this rule.

(b) LECs and CMRS providers are not required to comply with paragraph (a) for assets described above where the LEC or CMRS provider demonstrates, through the reporting requirement described below, that such compliance is precluded by:

- (1) Federal, state, tribal or local law;
- (2) Risk to safety of life or health; or
- (3) Private legal obligation or agreement.

(c) Within six months of the effective date of this requirement, LECs and CMRS providers subject to this section must file reports with the Chief of the Public Safety & Homeland Security Bureau.

- (1) Each report must list the following:
 - (i) Each asset that was designed to comply with the applicable backup power requirement as defined in paragraph (a);

- (ii) Each asset where compliance with paragraph (a) is precluded due to risk to safety of life or health;
- (iii) Each asset where compliance with paragraph (a) is precluded by a private legal obligation or agreement;
- (iv) Each asset where compliance with paragraph (a) is precluded by Federal, state, tribal or local law; and
- (v) Each asset that was designed with less than the emergency backup power capacity specified in paragraph (a) and that is not precluded from compliance under paragraph (b).

(2) Reports listing assets falling within the categories identified in paragraphs (c)(1)(ii) through (iv) must include a description of facts supporting the basis of the LEC's or CMRS provider's claim of preclusion from compliance. For example, claims that a LEC or CMRS provider cannot comply with this section due to a legal constraint must include the citation(s) to the relevant law(s) and, in order to demonstrate that it is precluded from compliance, the provider must show that the legal constraint prohibits the provider from compliance. Claims that a LEC or CMRS provider cannot comply with this section with respect to a particular asset due to a private legal obligation or agreement must include a description of the relevant terms of the obligation or agreement and the dates on which the relevant terms of the agreement became effective and are set to expire. Claims that a LEC or CMRS provider cannot comply with this section with respect to a particular asset due to risk to safety of life or health must include a description of the safety of life or health risk and facts that demonstrate a substantial risk of harm.

(3) For purposes of complying with the reporting requirements set forth in paragraphs (c)(1)(i) through (v), in cases where more than one asset necessary to maintain communications that are normally powered from local commercial power are located at a single site (*i.e.*, within one central office), the reporting entity may identify all of such assets by the name of the site.

(4) In cases where a LEC or CMRS provider identifies assets pursuant to paragraph (c)(1)(v), such LEC or CMRS provider must comply with the backup power requirement in paragraph (a) or, within 12 months from the effective date of this rule, file with the Commission a certified emergency backup power compliance plan. That plan must certify that and describe how the LEC or CMRS provider will provide emergency backup power to 100 percent of the area covered by any noncompliant asset in the event of a commercial power failure. For purposes of the plan, a provider may rely on on-site and/or portable backup power sources or other sources, as appropriate, sufficient for service coverage as follows: a minimum of 24 hours of service for assets inside central offices and eight hours for other assets, including cell sites, remote switches, and digital loop carrier system remote terminals. The emergency backup power compliance plans submitted are subject to Commission review.

(5) Reports submitted pursuant to this paragraph must be supported by an affidavit or declaration under penalty of perjury and signed and dated by a duly authorized representative of the LEC or CMRS provider with personal knowledge of the facts contained therein.

(6) Information filed with the Commission pursuant to subsection (c) of this rule shall be automatically afforded confidentiality in accordance with the Commission's rules.

(7) LECs that meet the definition of a Class B company as set forth in Section 32.11(b)(2) of the Commission's rules and non-nationwide CMRS providers with no more than 500,000 subscribers are exempt from this reporting requirement.

Several parties have filed Court Appeals of the FCC's Back-up Power Order.

Individuals/Organizations-to-Government

In the United States, 9-1-1 is the universal emergency number. Individuals call this number in an emergency to initiate action. On the other end of the phone are public safety answering points (PSAPs) that are manned by trained operators taking these calls. Information on 9-1-1 calls can be dynamic, complex, and confusing. Therefore, public safety communications professionals must be included in the planning effort to reach the best preparedness goals of this country.

Enhanced 9-1-1 (E9-1-1) addresses emergency calls made from wired and wireless (and typically mobile) phones, automatically reporting the telephone number and location of the E9-1-1 caller. The Alliance for Telecommunications Industry Solutions' Emergency Services Interconnection Forum (ATIS ESIF) generates and refines both technical and operational interconnection issues to ensure that life-saving E9-1-1 service is available for everyone in all situations. ATIS ESIF also enables many different telecommunications entities to fully cooperate and interconnect with each other to determine the best practices and solutions necessary to effectively and promptly deploy E9-1-1 services. Among the successes already realized by the group include [PSAP Documentation to Satisfy the Richardson Order Verification Requirement](#), [Standardized Wireless Carrier Procedures/Contact Lists Needed for PSAP 9-1-1 Call Investigations](#), and wireless Phase II Test Methodology. Additional works recently completed draft American National Standards for Trial Use include: ATIS-PP-0500002-200X, Emergency Services Messaging Interface; ATIS –PP-0500006-200X, EISI ALI Service; and ATIS-PP-0500007-200X, Emergency Information Services Interface (EISI) Implementation with Web Services.

The advent of Internet-based communications is providing a significant challenge in providing location and

telephone number information for emergency calls.⁹ Next Generation 9-1-1 (NG9-1-1) is a two-year project that is a collaborative effort between universities, industry, state and local governments, the National Emergency Number Association (NENA) and Internet2. Annex D provides a diagram that visually depicts the NG9-1-1 project. Standards are being developed for NG9-1-1 for requirements and basic design, service operations, and PSAP operational methods. These standards are consistent with NRIC 1B / 1D recommendations. They also need to be consistent with federal XML messaging standards and integrated with overall IP-based emergency communications structures.

The Research and Innovative Technology Administration (RITA) coordinates the U.S. Department of Transportation's (DOT) research programs and is charged with advancing the deployment of cross-cutting technologies to improve our Nation's transportation system. The Nation's current 9-1-1 system is designed around telephone technology and cannot handle the text, data, images and video that are increasingly common in personal communications and critical to future transportation safety and mobility advances. The [DOT's Next Generation 9-1-1 \(NG 9-1-1\)](#) initiative will establish the foundation for public emergency communications services in a wireless mobile society.

A NENA [initiative](#) is striving to ensure a coordinated and managed approach to the deployment of next-generation IP-based 9-1-1, or NG9-1-1, systems nationwide. As part of the initiative, NENA has created a Technical and Operations working group that will develop a plan to transition public-safety answering points, or PSAPs, to NG9-1-1 systems.

The Association of Public-Safety Communications Officials (APCO) International is working on a standard project for *Effective Practices for Wireless Calls*, as well as a joint project with NENA to develop a PSAP Survivability MATRIX.

Based upon these three methods of public emergency communications to government, the Workshop task group in this area developed the following matrix to capture existing standards.

⁹ NG9-1-1 Portal (<http://ng911.tamu.edu/>)

Standards Matrix for Individuals/Organizations-to-Government Emergency Communications

ACCESS POINT ⇨	POTS	Cell Phones	VoIP	SMS (Short Messaging System)
PSAP Personnel* (e.g., training, procedures, certification)		- ATIS-0500004 - ATIS-0500005		
3rd Party Call Center* (e.g., OnStar, ATX, TeleAid, TRS) Personnel Training & Certification		- ATIS-0500005		
Communication Devices	- TIA TR-30 - TIA-689-A-2003 (TR-41.1) - TR-41.3	- TIA TR-45 - TIA/EIA-2000 - TIA/EIA-136	- TIA TSB-146 (TR-41.4) -TIA-1057 (TR-41.4) - TIA TR-45 - TIA-2000-C - IETF ECRIT - IETF GEOPRIV - IETF SIP	- TIA TR-45 - TIA-637
Technical Infrastructure	- ATIS-PP-0500002-200X* - J-STD-025 - ATIS-1000678.2006	-ATIS-0500001 - ATIS ESIF Issue 30 - ATIS ESIF Issue 33 - ATIS-PP-0500002-200X* - ATIS-PP-0500006-200X* - J-STD-025 - J-STD-034 - J-STD-036	- ATIS-PP-0500002-200X* - ATIS-PP-0500007-200X* - TIA TR-30 - TIA-1001 (TR-30.1) - TIA-1066 - TIA-878 - TIA-2000-C - T1.724-2004 - IETF ECRIT - IETF GEOPRIV - IETF SIP	- TIA-637 - TIA-824

*These standards currently are undergoing the ATIS standards development process to become American National Standards.

Applicable to all categories in the table above:

- NFPA 1221: Standard for the Installation, Maintenance, and Use of Emergency Services Communications Systems (2007 Edition)

Table Key:

<u>Designation</u>	<u>Title</u>
ATIS-0500001	ATIS ESIF Technical Report - High Level Requirements for Accuracy Testing Methodologies (ESIF Issue 22)
ATIS-0500004	ATIS ESIF Recommendation for the Use of Confidence and Uncertainty for Wireless Phase II
ATIS-0500005	ATIS ESIF Standard Wireless Text Message Case Matrix
ATIS-PP-0500002-200X	ATIS ESIF Emergency Services Messaging Interface (<i>Trial Use</i> American National Standard)
ATIS-PP-0500006-200X	EISI ALI Service (<i>Trial Use</i> American National Standard)
ATIS-PP-0500007-200X	ATIS ESIF Emergency Information Services Interface (EISI) Implemented with Web Services (<i>Trial Use</i> American National Standard)
ATIS ESIF Issue 30	Call Delivery (End-to-End Functional Testing)
ATIS ESIF Issue 33	Maintenance Testing
ATIS 1000678.2006	LAES for VoP Technologies in Wireline Telecommunications Networks, Version 2
T1.724-2004	UMTS Handover Interface for Lawful Interception
TIA and ATIS J-STD-025	TIA Lawfully Authorized Electronic Surveillance
TIA and ATIS J-STD-034	Wireless Emergency Services (Phase 1)
TIA and ATIS J-STD-036	Wireless Emergency Services (Phase 2)
TIA TR-8	Mobile and Personal Private Radio Standards (<i>e.g.</i> , Project 25/34, Broadband data)
TIA TR-30	Multi-Media Access, Protocols and Interfaces
TIA-1001	Transport of TIA-825-A Signals over IP Networks
ANSI/TIA-689-A-2003	Telecommunications – Multiline Terminal Systems – PBX and KTS Support of Enhanced 9-1-1 Emergency Calling Service
TIA TSB-146	Telecommunications – IP Telephony Infrastructures – IP Telephony Support for Emergency Calling Service
ANSI/TIA-1057	Telecommunications – IP Telephony Infrastructures – Link Layer Discovery Protocol for Media Endpoint Devices
TIA-1066	Lawfully Authorized Electronic Surveillance for VoIP (cdma2000®)
TIA-878-B	VoIP for HRPD (B version awaiting publication)
TIA/EIA-2000-C	cdma2000® support for VoIP
TIA-637	Short Message Services (SMS) for Wideband Spread Spectrum Systems
TIA-824	Generic Broadcast Teleservice
TIA-136	EDGE/GPRS Air Interface
TIA TR-41	TIA TR-41, User Premises Telecommunications Requirements
TIA TR-41.1	TIA TR-41.1, Telephony Aspects of MLTS and VoIP Terminal Equipment (formerly Multiline Terminal Systems)
TIA TR-41.3	TIA TR-41.3, Analog and Digital Wireline Terminals (no E911 standards, but the place where they would be worked for POTS telephones)
TIA TR-41.4	TIA TR-41.4, IP Telephony Infrastructures
IETF ECRIT	Various documents that focus on individual-to-authority emergency services can be found at: http://www.ietf.org/html.charters/ecrit-charter.html . The framework document

provides a good starting point for further investigations, see <http://tools.ietf.org/wg/ecrit/draft-ietf-ecrit-framework/>.
IETF GEOPRIV Various documents that can be found at: <http://www.ietf.org/html.charters/geopriv-charter.html>; Work focuses on location information and location configuration
IETF SIP Although the entire SIP work itself is relevant it is important to highlight the SIP Location Conveyance work since it has high relevance for emergency calling, see <http://tools.ietf.org/wg/sip/draft-ietf-sip-location-conveyance/>. This document makes use of SIP and hence extends various other SIP features. Related SIP documents are referenced in that specification but are largely available from the following webpage: <http://www.ietf.org/html.charters/sip-charter.html>

Following an analysis of this standards matrix, the following gap areas for standards were identified:

- Service operation
- Authentication and access
- Location of caller
- Accessibility
- Interoperability (PSAPs, responding vehicles, i2 to i3)

A number of further challenges were identified by the task group for further exploration:

- Six enabling factors that require resolution for NG E9-1-1
 - Funding, Policy, Jurisdiction, Standards, Trials/demos, Education at all levels
- Transition issues, user buy-in, and funding for transition and maintenance of systems
- Incentives for PSAPs to adopt the standards that will reduce the gaps in the quality, consistency, and accessibility of E9-1-1 services
- Location of E9-1-1 “caller” (e.g., VoIP, wireless)
- Expectations of E9-1-1 callers (higher than capability)
- Multiple E9-1-1 calls for same incident
- Sharing networks (radio, voice, data)
- Requirements/standards and open interfaces
- Rural/urban dichotomy
- Universal adoption of standards
- By the time standard is developed/published, technology has changed
- Convergence of the “3-legs” of emergency communications

Government-to-Individuals/Organizations

The two Workshop meetings raised a number of key questions:

- How do you alert the public in the quickest time to cause them to “take action” to avert loss of life and property?
- What technologies are being used to do this, or could be used?
- How are the needs of persons with disabilities and non-native language speakers being addressed?

A number of initiatives seek to address these questions:

FEMA Disaster Management eGov Initiative

- Provide the capability to share incident information horizontally and vertically
- Provide free basic incident management tools
- Ensure response staff is trained and experienced in using these tools
- Encourage a culture that promotes information sharing
- Create a practitioner-driven, public-private partnership to produce information exchange standards relating to incident management
- Provide a single source of access to information and services relating to disasters
- Enhance the nation’s ability to cope with incidents by increasing the ability to share information during emergencies
- Incident management data standards
- National standards driven by practitioners, not Federal agencies

Wireless Emergency Alert Systems

The Warning, Alert and Response Network (WARN) Act¹⁰ will:

- enable any Federal, State, tribal, or local government officials with credentials issued by the National Alert Office under section 103 to alert the public to any imminent threat that presents a significant risk of injury or death to the public;
- be flexible enough in its application to permit narrowly targeted alerts in circumstances in which only a small geographic area is exposed or potentially exposed to the threat;
- transmit alerts across the greatest possible variety of communications technologies, including digital and analog broadcasts, cable and satellite television, satellite and terrestrial radio, wireless communications, wireline communications, and the Internet to reach the largest portion of the affected population.

Based on Congressional guidance from the WARN Act, the FCC created the Commercial Mobile Service Alert Advisory Committee ([CMSAAC](#)). CMSAAC's mission was to develop recommendations on technical

¹⁰ Security and Accountability For Every Port Act of 2006 (SAFE Port Act), Pub.L. 109-347, Title VI-Commercial Mobile Service Alerts (WARN Act).

standards and protocols to facilitate the ability of commercial mobile service (CMS) providers to voluntarily transmit emergency alerts to their subscribers. On December 14, 2007, the FCC issued a Notice of Proposed Rulemaking (NPRM), [PS Docket No.07-287](#), based on the recommendations from the CMSAAC. In the NPRM the FCC initiated a comprehensive rulemaking to establish a Commercial Mobile Alert System (CMAS), under which Commercial Mobile Service providers may elect to transmit emergency alerts to the public. This proceeding represents the FCC's next step in compliance with the WARNAct requirement that the Commission enable commercial mobile service alerting capability for providers that elect to transmit emergency alerts. In addition, with this rulemaking the FCC continues to address its obligations under the President's "Public Alert and Warning System" [Executive Order](#) that the Commission "adopt rules to ensure that communications systems have the capacity to transmit alerts and warnings to the public as part of the public alert and warning system."¹¹ SDOs are already scheduled to meet to start to address CMSA standards issues. Joint ATIS WTSC G3GSN/TIA TR45.2 meeting on standards for CMAS was held January 22-23, 2008 in San Diego.

Mobile Wireless Broadband for Public Protection and Disaster Relief (PPDR) and Intelligent Transportation Systems

- Many agencies have their own communications systems
 - Proprietary equipment
 - Different bands
 - Different protocols
 - Inconsistent capabilities for voice and data
- Problem compounded across adjoining jurisdictions that need to cooperate
- Biggest issues:
 - Lack of interoperability
 - An inconvenience for routine operations
 - A potential calamity in emergencies
 - Limited spectrally efficiency
 - Limits the data rates available –precious time wasted for large downloads
 - Limits number of users supported, particularly during emergencies
 - Increases CapEx and OpEx of Public Safety networks
- Requirements:
 - Immediate, wide-area, high-speed communications
 - Ability to supplement or replace primary communication networks
 - Provide stationary and mobile communications
 - Flexible, familiar user-interface
 - Standard terminal equipment and application software

¹¹ See *Public Alert and Warning System*, Exec. Order No. 13,407, 71 Fed. Reg. 36975 (2006) (*Executive Order*), §3(b)(iii).

- Flexible, multi-tiered command and control structure

Recommends Mobile Broadband Wireless Access (BWA) with VoIP

- Provides a consistent, robust capability that
 - Works for all routine operations
 - Provides priority for emergency operations
- Provides high-speed access to data, including private Internet sites
 - Graphical, text, or speech output
 - Commercial vehicle cargo (especially hazmat)
 - Building floor plans for firefighters
 - Medical data for ambulances
 - Vehicle (and other) records for police
 - Maps and facility records for major emergencies and evacuation
- Can be installed for public authority communications
 - Police, fire, ambulance
 - Traffic authorities
 - Bus and trains
 - Collect / provide information to the public

Provided data on current standards status for BWA

Integrated Public Alert and Warning System ([IPAWS](#))

- IPAWS is:
 - A DHS-sponsored program to improve public alert and warning
 - System of warning systems (includes both current & new systems)
- DHS led, in coordination with the Federal Communications Commission (FCC), the National Oceanic and Atmospheric Administration (NOAA), and others
- Congress provided \$20 million to improve public warning
- Coordinated with White House Task Force on Effective Warning, co-chaired by DHS and NOAA
 - Digital Emergency Alert System (DEAS) Pilot
 - Geo-Targeted Alerting System (GTAS)
 - DHS Web Alert Relay Network (DHS WARN)
 - All-Hazard Web Alert Portal (AWAP) Pilot
 - Emergency Alert System (EAS) satellite and network upgrade
 - NOAA network upgrades and all-hazards radios in public schools
 - Reports, IPAWS architecture, exercises, and public education
- END STATE: A technologically enhanced public warning system that:
 - Provides DHS, State, and local officials with multiple means to provide the general public with timely alert and warning
 - Serves people with disabilities and those who do not speak English
 - Improves security, addressability, reliability, and survivability
 - Uses international standards and non-proprietary solutions
 - Leverages public/private partnerships for cost-effective solutions

- Provides effective warning at all times, in all places, over multiple media
- Develop and execute evolving IPAWS architectures, tests and exercises, and other evaluations
- Empower, educate, and protect the public

IPAWS will improve public safety through the rapid dissemination of emergency messages to as many people as possible over as many communications devices as possible. To do this, IPAWS expands the traditional alert and warning system to include more modern technologies. At the same time, FEMA is upgrading the alert and warning infrastructure so that no matter what the crisis is, life-saving information will get to the public -day or night, at home, at work, at school or even on vacation.

In March 2007, the GAO issued a report: *Emergency Preparedness - Current Emergency Alert System Has Limitations and Development of a New Integrated System Will Be Challenging*, [GAO-07-411](#). In its report the GAO concluded:

The ability to communicate reliable emergency information to the public is critical during disasters, and effective emergency warnings allow people to take actions that could save lives and property. While EAS is one of the mainstays of the nation's capacity to issue such warnings, its reliability is uncertain. With no requirements to test the relay system for disseminating national alerts and with no nationwide test results—apart from the partial test conducted in January 2007, in which three primary relay stations failed to transmit or receive the emergency message—the public lacks assurance that the system would work in a national emergency. Although several federal initiatives are underway to integrate existing warning systems and FEMA is planning to nearly double the number of primary relay stations in order to increase the system's redundancy, these initiatives have just begun to receive funding and are likely to take years to implement. In the meantime, questions remain about the reliability of EAS's relay system.

Adequate training for all EAS participants is critical to ensure that they are qualified to use the equipment and to draft effective emergency messages that the public will be able to understand and act on appropriately. Despite the federal government's efforts to integrate and improve EAS, the system will be ineffective if the public ignores alerts or does not take appropriate action based on the information provided.

Effectively implementing an integrated alert system will require collaboration among a broad spectrum of stakeholders, including those at the federal, state, and local levels; private industry; and the affected consumer community. FEMA believes that the effective execution of the public alert and warning system requires consulting, coordinating, and cooperating with diverse stakeholders. However, a regular forum for public and private stakeholders to discuss emerging issues related to the implementation of the integrated alert system does not exist. Without such a forum, coordination among the diverse stakeholders could occur on an ad hoc basis, but there would be no systematic means of bringing all interested public and private stakeholders together for a comprehensive, strategic review of the processes, standards, systems, and strategies related to the implementation of the integrated public alert and warning system.

GAO recommended Executive Action:

To ensure that the Emergency Alert System is capable of operating as intended and that coordination with a variety of stakeholders on the implementation of the integrated public alert and warning system exists, we recommend that the Secretary of Homeland Security direct the Director, FEMA, to work in conjunction with the Chairman, FCC, to take the following actions:

- Develop and implement a plan to verify (1) the dependability and effectiveness of the relay distribution system, which is used to disseminate national-level EAS alerts, and (2) that EAS participants have the training and technical skills to issue effective EAS alerts.
- Establish a forum for the diverse stakeholders involved with emergency communications to discuss emerging and other issues related to the implementation of an integrated public alert and warning system. Representation on the forum should include relevant federal agencies, state and local governments, private industry, and the affected consumer community.

DHS also has the Homeland Security Advisory System ([HSAS](#)) to provide emergency information to the public. The Homeland Security Advisory System is designed to guide our protective measures when specific information to a particular sector or geographic region is received. It combines threat information with vulnerability assessments and provides communications to public safety officials and the public. This system was established in [Homeland Security Presidential Directive 3](#).

The FCC has also held several Summits to focus on Emergency Communications:

- The FCC convened disability organizations, service providers, government agencies and other stakeholders on March 25, 2004, for a day-long summit to discuss “[Emergency Communications and Homeland Security -- Working with the Disability Community](#).” The [Summit](#) focused on identifying communications barriers faced by people with disabilities during national emergencies or terrorist attacks and developing strategies for resolving them where possible. The summit fulfilled one of the action items identified on the FCC’s Homeland Security Action Plan, announced by FCC Chairman Michael K. Powell on July 10, 2003. Chairman Powell addressed summit attendees and highlighted the importance of promoting access to effective communications services by all Americans, particularly in emergency situations.
- The FCC held an [E9-1-1 Disability Access Summit](#) to focus on E9-1-1 calling and access for persons with hearing and speech disabilities on Wednesday, November 15, 2006. In 2005, the Commission initiated a proceeding seeking comment on how the Commission can ensure that consumers using Internet-based forms of Telecommunications Relay Services (TRS), specifically Video Relay Services (VRS) and Internet Protocol Relay (IP Relay), can access emergency services in the same way as all other consumers. *In the Matter of Telecommunications Relay Services and Speech-to-Speech for Individuals with Hearing and Speech Disabilities*, FCC 05-196, 20 FCC Rcd 19,476

(2005). Internet-based TRS calls do not originate on the PSTN and therefore present unique challenges. The [E9-1-1 Disability Access Summit](#) was intended to provide an opportunity to explore challenges and potential solutions for users of Internet-based TRS services to access Public Safety Answering Points (PSAPs) by calling 9-1-1.

- The Federal Communications Commission’s Public Safety and Homeland Security Bureau (PSHSB) held a [Summit on Communications Network Surge Management in Emergencies](#) on Tuesday, September 25, 2007. The [Summit](#) examined how communications networks are managed during mass emergency situations, as well as what the public can do to help ensure that they are able to effectively use their wireless commercial devices during such incidents.

The [Joint Advisory Committee on Communications Capabilities of Emergency Medical and Public Health Care Facilities](#) (“Joint Advisory Committee”) was established by the Chairman of the Federal Communications Commission and the Assistant Secretary for Communications and Information, U.S. Department of Commerce pursuant to the *Implementing Recommendations of the 9/11 Commission Act of 2007* (the “Act”). The Joint Advisory Committee’s mission is to examine the communications capabilities and needs of emergency medical and public health care facilities. Specifically, the Joint Advisory Committee is to assess:

- Specific communications capabilities and needs of emergency medical and public health care facilities, including the improvement of basic voice, data, and broadband capabilities;
- Options to accommodate growth of basic and emerging communications services used by emergency medical and public health care facilities; and
- Options to improve integration of communications systems used by emergency medical and public health care facilities with existing or future emergency communications networks.

The Joint Advisory Committee reported its findings to the Senate Committee on Commerce, Science, and Transportation and the House of Representatives Committee on Energy and Commerce, recommending:

1. Policymakers encourage the deployment of interoperable, standards-based broadband networks built on common and standardized Internet Protocols that can transmit bandwidth-intensive information such as video and graphics in a rapid, reliable, and secure manner.
2. Congress establish a federal interagency coordinating committee on emergency communications systems to establish strong, consistent national (federal) guidance, standards and direction to insure consistent development of compatible communication systems across the nation.
3. The federal government renew its commitment to develop, harmonize, and ensure widespread adoption of shared standards and protocols.
4. Federal and state agencies develop common criteria for all contracts and grants supporting emergency communications.

5. Greater coordination, investment, and utilization of telemedicine technologies for both day-to-day and emergency response.
6. Better coordination between existing systems to be able to share and analyze real-time data across systems and provide better communications during times of emergency.
7. The Department of Homeland Security lead an effort to create and coordinate a geospatial Command and Coordination System, based on open enterprise architecture, to allow common patient and emergency vehicle tracking for better situational awareness for all Emergency Medical and Public Health Care Facilities.
8. First responders, health care personnel, and patients have ubiquitous access to broadband services and applications by fostering a regulatory environment in which private sector companies build robust broadband networks and providing targeted funding.

George Washington University (GWU) also held a two-day event on emergency communications, the [*National Conference on Emergency Communications \(NCEC\)*](#) on December 12-13, 2005. This conference featured some thirty different speakers selected from the federal as well as state and local governments, a wide range of industry spokespeople, several professional societies, relief organizations and NGOs, universities, and other interested parties. There were thirty different sponsors including the ANSI-HSSP. A [*White Paper*](#), drawing on a number of sources including presentations at the National Conference on Emergency Communications (NCEC) was produced. The sponsors are also listed in the Appendices attached to the White Paper report. This White Paper also includes elements drawn from relevant Web sites and many other documents prepared by concerned academic, standards and industry organizations who have offered information and recommendations about emergency communications as well as warning and recovery efforts in the wake of Hurricane Katrina, the Pakistan Earthquake and the Asian Tsunami.

During the ANSI-HSSP Workshop meetings, the following standards / initiatives were identified as playing a key role in the government-to-individuals/organizations emergency communications sphere:

Developer / Source	Designation	Title	Description/Scope
FEMA	IPAWS	<i>Integrated Public Alert and Warning System</i>	May 2008 National incremental roll-out begins
FCC /OASIS, TIA and others	CMAS	<i>Commercial Mobile Alert System</i>	CMSAAC made recommendation that the CMAS use CAP as the basic alerting protocol from the alert initiator to the alert gateway. TIA and others who develop cellular standards are likely to develop CMAS standards. FCC NPRM, PS Docket No.07-287 . Joint ATIS WTSC G3GSN/TIA TR45.2 meeting on standards for Commercial Mobile Alert Service (CMAS) is scheduled to be held January 22-23 in San Diego.
FCC / OASIS	EAS / CAP	<i>Review of Emergency Alert System (EAS)</i>	2 nd Report and Order and Further NPRM, July 2007, EB Docket No. 04-296 . FCC requires use of Common Alerting Protocol (CAP), if adopted by FEMA. Cap v1.1 was developed by the Organization for the Advancement of Structured Information Standards (OASIS), a non-profit, international consortium that develops standards. See http://www.oasis-open.org/home/index.php .
CEA	CEA-608	Line 21 Data Services	How to transmit and receive EAS and NOAA alerts via line 21 of NTSC video.
CEA	CEA-2009	Receiver Performance Specification for Public Alert Receivers	How to receive alert messages via NOAA Weather Radio
CEA	NRSC-4	US RBDS Standard	How to transmit and receive FCC EAS messages via FM RDS subcarrier
CEA	ATSC-A/65B	Program and System Information Protocol for Terrestrial Broadcast and Cable	Defines method for sending messages intended for a specific county or portion of a county
CEA/SCTE	ANSI-J-STD-042-	Emergency Alert Message for Cable	

Developer / Source	Designation	Title	Description/Scope
	2002 (also SCTE 18 2002)		
Multi-Technical Services and Cell Broadcast Technologie	CellAlert EAS-2	Interface Decoder	Jointly developed by Multi-Technical Services and Cell Broadcast Technologies. The decoder allows cellular provider networks, with cell-broadcast messaging capability, to instantly send EAS information to subscribers in, or entering, a designated warning location.

The key issues/challenges identified in this area included:

- Does not appear to be single consensus on a National Architectural approach, thus, many things are being considered.
- SMS is not a good choice for wide-scale, time-sensitive alerts. Point-to-point communications are not as effective and point-to-multipoint, broadcast-type communications. High volume SMS also have been blocked by some service providers as SPAM.
- Some wide-area broadcast technique is best, but various technology views, NOAA exists, satellites have large footprint but signal does not penetrate as well, cell Broadcast with enhancements technically can work, but not widely used now.
- Experimental system data feedback desired.
- The need for better alerting systems that will cause folks to take action, and are secure and reliable.
- Must consider persons with disabilities and language issues or we are not alerting all individuals.

Cell Broadcast EAS Issues:

- Standards exist, commercial products do not
- Would require change out of handsets (all CDMA; some GSM)
- Existing GSM Cell Broadcast technology reduces battery “talk time”
- Interface from Cell Broadcast Center to BSC not standardized or developed
- High Carrier Involvement: wireless carrier would have to parse EAS messages and distribute them to the appropriate cell sites as required
- Message length limited (256 characters for CDMA & 93 for GSM)
- High cost and no revenue potential by itself (message sent to all handsets and acknowledged by none) – ETSI reports that this is a barrier to deployment in Europe

Conclusion

Many of the issues raised during the two ANSI-HSSP Emergency Communications Workshop meetings required policy guidance from government. As can be seen from events since this Workshop was conducted, significant government activity has occurred focused on the three legs of emergency communications reviewed at the Workshops. This has included several FCC Summits, passage of the WARN Act, creation of the DHS Office of Emergency Communications, passage of *Implementing Recommendations of the 9/11 Commission Act of 2007*, issuance of Executive Orders 13407 and 13347, the FCC's EAS Order in [EB Docket No. 04-296](#) and CMAS NPRM in [PS Docket No.07-287](#), and NG911 activities and IPAWS trials. After the FCC concludes its decision making, Standards Development Organizations (SDOs) will also be able to develop the standards for CMAS. A Joint ATIS WTSC G3GSN/TIA TR45.2 meeting on standards for Commercial Mobile Alert Service (CMAS) was also held.

Although the CMSAAC looked at issues related to the special needs of persons with disabilities and non-English speakers, both of these areas probably need further investigation. Further recommendations may come from the *Interagency Coordinating Council on Emergency Preparedness and Individuals with Disabilities (ICC)* and a proposed future ANSI-HSSP Workshops devoted to emergency preparedness for persons with disabilities and special needs. There may be standards needs as well from the *Joint Advisory Committee on Communications Capabilities of Emergency Medical and Public Health Care Facilities*. DHS needs to finish its roll out of IPAWS and the FCC needs to conclude its EAS and CMAS and Back up power proceedings.

The fourth leg of Emergency Communications, "government-to-government" communications was determined to be outside the scope of the ANSI-HSSP Workshop which focused more on the private sector and the needs of citizens and individuals and organizations, however a lot of activity has occurred recently in this area. For the purpose of information sharing, Annexes C and F summarize some of that activity and provides links to more information.

Annex A – Participation

Two in-person workshop meetings were held for this workshop:

December 1-2, 2004
December 14-15, 2005

Hosted by Motorola (Schaumburg, IL)
Hosted by NIST (Gaithersburg, MD)

Additionally, conference calls and e-mail communications were used to facilitate and collect the workshop participants' input. The following organizations supplied experts to one or more of these workshop meetings:

Alert Systems, Inc.
Alliance for Telecommunications Industry Solutions (ATIS)
American Council of the Blind
American National Standards Institute (ANSI)
ArrayComm, LLC
Association of Public-Safety Communications Officials (APCO) International
BearingPoint
Bell Mobility
Cellular Telecommunications and Internet Association (CTIA)
Cingular Wireless
COMCARE
Community Emergency Preparedness Information Network (CEPIN) Telecommunications for the Deaf and Hard of Hearing, Inc.
Dialogic Communications Company
Dynainfo
EDS
Ericsson Inc.
Federal Communications Commission (FCC)
Gallaudet University
Harris Corporation
Hughes Network Systems
IHS/Global
Industry Canada
Infinite Global Infrastructures, LLC
Information Age Economics (IAE)
Institute of Electrical and Electronics Engineers, Inc. (IEEE)
Intrado Inc.
Kontek Industries
Level 3 Communications, LLC
Library of Congress, Congressional Research Service
Lockheed Martin

LogicaCMG, Global Telecoms
Lucent Technologies
Motorola, Inc.
MVLabs LLC
National Electrical Manufacturers Association
National Emergency Number Association (NENA)
National Fire Protection Association (NFPA) 1600 Technical Committee
National Institute of Standards and Technology (NIST)
National Telecommunications and Information Administration (NTIA)
NOAA National Weather Service
Nortel PEC
Office of the Secretary of Defense (OSD)
Pacific Northwest National Labs (PNNL)
Personal Alarm Systems (PAS)
Satellite Industry Association (SIA)
Science Applications International Corporation (SAIC)
Send Word Now Communications
Society of Cable Telecommunications Engineers (SCTE)
South Carolina Budget & Control Board, Division of the State CIO
Sprint Nextel
Telecommunications Industry Association (TIA)
The JED Group, LLP
The Safe America Foundation
T-Mobile
U.S. Access Board
U.S. Department of Commerce
U.S. Department of Homeland Security (DHS) – Science and Technology Directorate
U.S. DHS - Federal Emergency Management Agency (FEMA)
U.S. DHS - National Cyber Security Division (NCSD)
U.S. DHS - NIMS Integration Center (NIC)
U.S. DHS - Office for Domestic Preparedness (ODP)
U.S. Food and Drug Administration/Health and Human Services
U.S. General Services Administration (GSA)
U.S. Nuclear Regulatory Commission
Underwriters Laboratories (UL)
Urban Health Inc
Verizon
VIACK Corporation
Wheelock, Inc.
WI3N
Ygomi LLC

Annex B – Global Standards Collaboration

The major communications sector standards organizations gather periodically at an event called [Global Standards Collaboration](#) (GSC). Those organizations who participate on a regular, recurring basis are called Participating Standards Organizations (PSOs), and currently consist of:

- [TIA](#) and [ATIS](#) (USA)
- [ETSI](#) (EU)
- [ISACC](#) (Canada)
- [TTA](#) (Korea)
- [TTC](#) and [ARIB](#) (Japan)
- [ACIF](#) (Australia)
- [CCSA](#) (China)

[ITU-T](#) and [ITU-R](#) participate regularly, and other groups that have been invited and participated include: [ANSI](#), [JTC-1](#), [IETF](#), [ATMF](#), [IEEE](#), [SCTE](#), [APT](#), [CITEL](#), [IEC](#), [ISO](#), [ITSA](#).

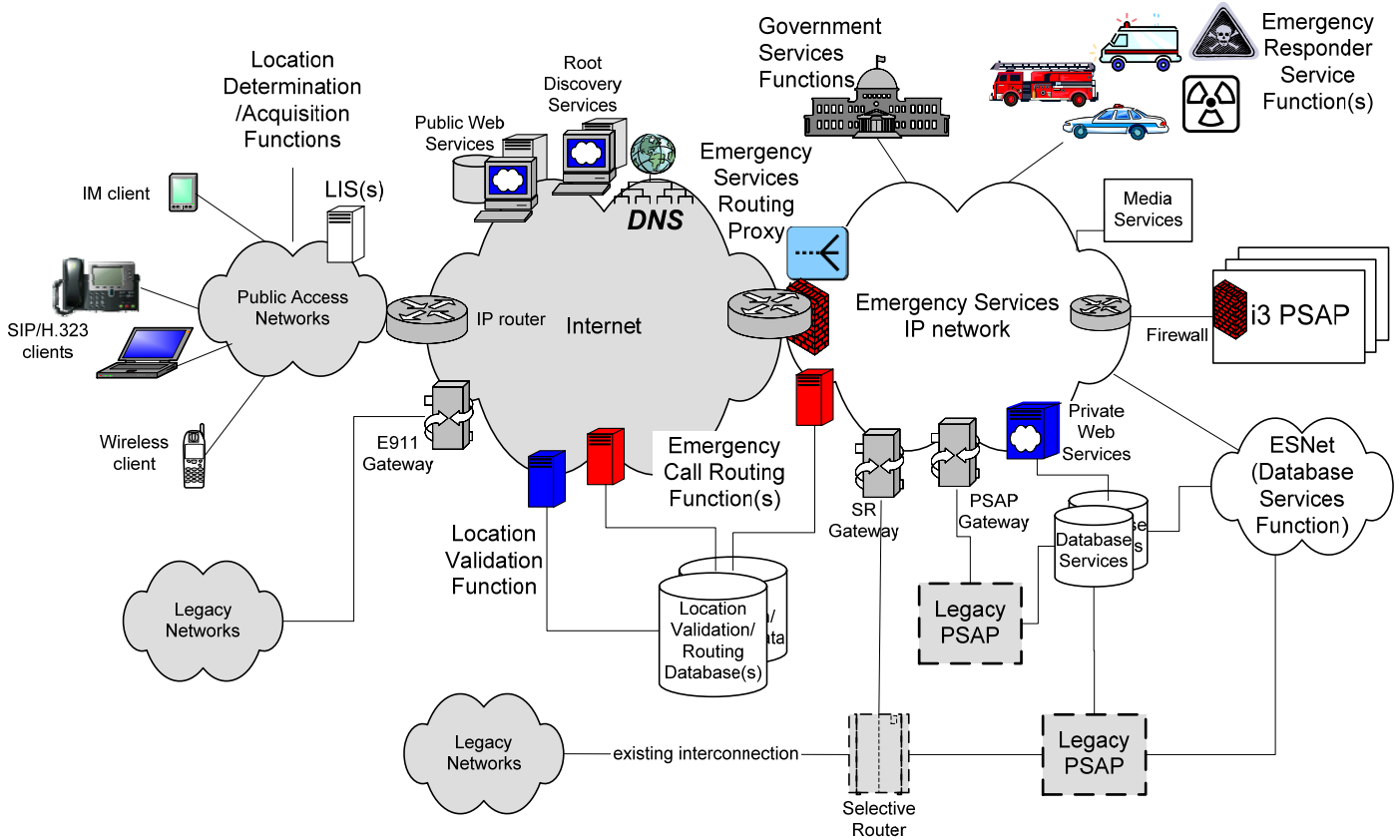
For more information on the GSC, please visit its website: www.gsc.etsi.org

Annex C – Government-to-Government Emergency Communications

The following initiatives are among those addressing various aspects of the government-to-government leg of emergency communications:

- NIST/DHS Public Safety Interoperability Workshops
- [SAFECOMM Office of DHS](#)
- [AGILE \(Advanced Generation of Interoperability for Law Enforcement\) Program](#)
- [Project 25](#) and other work in [TIA TR-8](#)
- [National Public Safety Telecommunications Council \(NPSTC\)](#)
- [Public Safety Wireless Advisory Committee \(PSWAC\)](#)
- [National Task Force on Interoperability](#)
- User organization groups such as [APCO](#), [NASTD](#), and the [Federal Law Enforcement Wireless Users Group \(FLEWUG\)](#)
- Internationally at [ITU](#), Project MESA, [GSC](#), etc.

Annex D - NENA NG9-1-1 Design (with IETF)



Annex E – Glossary of Terms and Acronyms

Note: Acronyms used are provided due to either being used in this Workshop report or as an attempt to visually show the kinds of emergency communications that are available and being used.

- ANSI: American National Standards Institute
- APCO: Association of Public-Safety Communications Officials
- ARS: Amateur Radio Services
- CATV: Cable Television
- Citizen: Includes private individuals or organizations
- CMRS: Commercial Mobile Radio Services
- CSRIC: Communications, Security, Reliability and Interoperability Council
- CtoCvS: Citizen to Citizen via SMS/text
- CtoCvWoM: Citizen to Citizen via Word of Mouth
- CMAS: Cellular Mobile Alert Service
- CWIN: CIP & Cyber Warning Information Network
- Emergency Communications: Encompassing of all forms and services available to governments and citizens
- Emergency Telecommunications: Including telecommunication infrastructure transmission & reception and the variety of emergency and priority communications services concerning public, dedicated and private telecommunications networks (*i.e.*, NS/EP ETS)
- ENA: Emergency Number Access (*i.e.*, 9-1-1, E9-1-1, E1-1-2, E1-1-9, etc.)
- EBS: Emergency Broadcasting System
- ETS: Emergency Telecommunications Service (NS/EP)
- ETSI: European Telecommunications Standards Institute
- EMTEL: ETSI Emergency Telecommunications
- GASvE: Government Alert Service via Email
- GASvH: Government Alert Service via Highway
- GASvS: Government Alert Service via SMS
- GETS: Government Emergency Telecommunications Service (NS/EP)
- GMDSS: Global Maritime Distress and Safety System
- Government: Appropriate authority and/or organizations providing emergency or other response services (NS/EP)
- IPAWS: Integrated Public Alerts and Warning System
- IPS: Internet Priority Service (NS/EP)
- LAES: Lawfully Authorized Electronic Surveillance (NS/EP)
- NCAS: National Cyber Alert System
- NECP: National Emergency Communications Plan
- NENA: National Emergency Number Association
- NETS: Nationwide Emergency Telecommunications Service (NS/EP)
- NS/EP: National Security/Emergency Preparedness
- OEC: DHS Office of Emergency Communications

- Project MESA: Public Safety Int'l Partnership for Broadband Capabilities, Mobility for Emergency and Safety Applications
- PRS: Private Radio Services (*e.g.*, P25, Tetra)
- PSAP: Public Safety Answering Point
- PSECS: Public Schools Emergency Communications System
- PSO: Public Safety Officers and Participating Standards Organization
- PSWIN: Public Safety Wireless Network
- PSTN: Public Switched Telephone Network
- SAFECOM/AGILE: US Government programs addressing public safety communications issues (*i.e.*, interoperability)
- SASvE: School Alert Service via Email
- TsecEmCom: Transportation-sector Emergency Communication systems (*e.g.*, Amber Alert on Highway Sign)
- TDR: Telecommunications for Disaster Relief (ITU-T)
- TSP: Telecommunications Service Priority (NS/EP)
- VoIP: Voice over Internet Protocol
- WPS: Wireless Priority Service

Annex F – Additional Resources for Government-to-Government Emergency Communications

The fourth leg of the Global Standards Collaboration (GSC) Emergency Communications resolution was specifically excluded from the two ANSI HSSP Workshops since so much other activity was directed at this important aspect of Emergency Communications and the needs of first responders. While in-depth cover of this important area is also outside of the scope of this ANSI-HSSP Emergency Communications Workshop report, a summary of some of recent activities and sources of information is being provided in this Annex for completeness and to assist Workshop attendees in finding more information.

Some of the activities include the work of NPSTC, DHS SAFECOM, DHS Office of Emergency Communications (OEC), Project 25, MESA, TIA TR-8, NSTAC Emergency Communications and Interoperability Task Force (ECITF), a FCC Summit: [First Responders Summit: Interoperable and Reliable Public Safety Communications](#), APCO, and the National Conference on Emergency Communications (NCEC). From a standards perspective, TIA is the principal SDO developing standards in North America for use by public safety users for mission-critical government-to-government communications. This includes work in TIA TR-8 for narrowband, wideband, and broadband public safety communications, (*i.e.*, data, voice, video), related conformity assessment activities for Project 25, MESA, and the use of cdma2000[®] technology for public safety applications, as well as satellite communications. TIA has numerous groups in its standards program as well as activities in the trade association, focusing on the needs of public safety users both from a standards, spectrum, conformity assessment, and grants and funding perspective.

FCC

The FCC's Public Safety and Homeland Security Bureau (PSHSB) held a [First Responders Summit: Focus on Public Safety Communications](#) on Friday, April 20, 2007. The Summit included expert panels composed of representatives from the public safety community, government, and the communications industry. In addition, the [Summit](#) closed with a roundtable discussion on key issues related to emergency preparedness and response. The agenda included three expert panel discussions:

- Panel One: Federal Government Programs and Initiatives for Public Safety
- Panel Two: Disaster Communications Planning for First Responders
- Panel Three: New Technologies and Applications in Emergency Communications

Communications Security, Reliability, and Interoperability Council (CSRIC)

The FCC has chartered the CSRIC (replaces the Network Reliability and Interoperability Council (NRIC), and Media Security and Reliability Council (MSRC). The CSRIC's duties will include:

1. recommending to the FCC best practices to ensure the security, reliability, operability and interoperability of public safety communications systems;
2. evaluating ways to strengthen the collaboration between communication service providers and public safety agencies during emergencies;
3. recommending to the FCC ways to improve the Emergency Alert System (EAS), including best practices for EAS;
4. recommending to the FCC steps necessary to better prepare for shifts in communications usage patterns that likely would result from a pandemic flu outbreak;
5. recommending to the FCC technologies and systems that can best facilitate the communication of emergency information to and from hospitals, schools, day care facilities and other facilities that provide vital public services;

6. developing and recommending to the FCC best practices to facilitate the communication of emergency information to the public, including people who do not speak English, individuals with disabilities, the elderly and people living in rural areas;
7. recommending to the FCC methods by which the communications industry can reliably and accurately measure the extent to which key best practices are implemented;
8. reviewing and recommending to the FCC updates of existing NRIC and MSRC best practices;
9. reviewing the deployment of Internet Protocol (IP) as a network protocol for critical next generation infrastructure, including emergency/first responder networks; and
10. reviewing and recommending to the FCC an implementation plan for the “emergency communications internetnetwork” advocated by NRIC VII, Focus Group 1D in its December 2005 Final Report.

9/11 Act, PL 110-53

The 9/11 Act mandates a [FCC vulnerability assessment](#) of the Nation's critical communications and information systems infrastructure and shall evaluate the technical feasibility of creating a [back-up emergency communications system](#) that complements existing communications resources and takes into account next-generation and advanced communications technologies. The FCC issued a Paperwork Reduction Act notice to enable the Commission to fulfill its obligation under the Implementing Recommendations of the 9/11 Commission Act of 2007 (Act), Public Law 110-53.

FCC has advised information will be sought concerning emergency communications networks, including user devices, network equipment, operations processes and operations systems, and concerning the feasibility of commercial service providers to support the needs of public safety, including:

- (1) technical capabilities and characteristics of equipment (*e.g.*, analog/digital, power, range, access protocol, broadband/wideband/narrowband, etc.),
- (2) technical capabilities and characteristics of commercial services to support the needs of public safety,
- (3) cost and deployment of commercial services for use by public safety,
- (4) cost of user devices and network equipment of emergency communications networks (*e.g.*, unit cost, maintenance/upgrade cost, etc.), and the cost of operations and operations systems (including feature upgrades) for emergency communications networks and services,
- (5) deployment of user devices, network equipment, and operations processes and equipment of emergency communications systems (*e.g.*, type of systems deployed or to be deployed), number of units deployed/sold, etc.),
- (6) standardization of user devices, network equipment, and operations interfaces of emergency communications systems (*e.g.*, standard/proprietary, standard activities, etc.),
- (7) interoperability (*i.e.*, the ability of communications among different systems, devices and groups) of user groups, user devices, network equipment, and operations processes and equipment of emergency communications systems (*e.g.*, interoperability among first responders within a jurisdiction, among jurisdictions using the same and different network technologies),
- (8) spectrum usage of user devices and network equipment of emergency communications systems (*e.g.*, frequencies of operation, shared/dedicated spectrum, etc.),
- (9) applications and application requirements for end users and the technical requirements for such applications including bandwidth needs,

- (10) operations systems features and operations processes supporting emergency network operation during an emergency,
- (11) service capabilities (*e.g.*, voice, data, video, mobile to mobile communications, etc.),
- (12) evolutionary trend of user devices, network equipment, and operations of emergency communications systems (*e.g.*, next generation, migration path, etc.),
- (13) backhaul connectivity of network equipment and facilities (*e.g.*, commercial/private, wired/wireless, capacity, etc.),
- (14) description of network technology and architecture (*e.g.*, whether the network design accommodates access to emergency responders from other jurisdictions, capability of architecture to support resiliency in disaster situations, etc.),
- (15) operations budget for the network,
- (16) responsibilities of the organizations operating the networks, including service provisioning, traffic management and network maintenance, especially during an emergency,
- (17) plans, if any, for restoring emergency communication services or reverting to backup networks in the event that a primary emergency communications network is damaged or destroyed,
- (18) ability of existing emergency communications networks to back up or complement the communication resources of other emergency communications networks,
- (19) ability to rapidly increase emergency communication network capacity in the event that the capacity limits of the network are exceeded in a major disaster,
- (20) a description of the role of "core services" such as authentication and agency locator services, whether and how they are implemented in existing and planned networks, and their costs,
- (21) a description of the processes and systems used or planned to connect emergency responders to a back-up network in an emergency, and
- (22) plans to restore emergency communications services if the network over which they are provided is damaged, destroyed, or sufficiently congested to be impaired or unusable (*e.g.*, changes in operations staffing in emergency conditions, dynamic bandwidth allocation to users or networks, back-up communications for other emergency communications services or networks), other administrative or planning issues associated with the deployment and maintenance of such backup national emergency communications capabilities.

FCC 700 MHz Decision

In a [Second Report & Order \(Order\)](#) adopted July 31, 2007, the Federal Communications Commission (FCC) revised the 700 MHz band plan and service rules to promote the creation of a nationwide interoperable broadband network for public safety and to facilitate the availability of new and innovative wireless broadband services for consumers. The 700 MHz Band spectrum, which runs from 698-806 MHz, currently is occupied by television broadcasters and will be made available for other wireless services, including public safety and commercial services, as a result of the digital television (DTV) transition. The Digital Television and Public Safety Act of 2005 (DTV Act) set a firm deadline of February 17, 2009, for the completion of the DTV transition.

In implementing Congress' directive to reallocate the airwaves, the Commission is focused on serving the public interest and the American people. The service rules the Commission adopts today help create a national broadband network for public safety that will address the interoperability problems of today's system, provide for a more open wireless platform that will facilitate innovation and investment, and facilitate the emergence of next generation wireless broadband services in both urban and rural areas. The

Order establishes a framework for a 700 MHz Public Safety/Private Partnership between the licensee for one of the commercial spectrum blocks and the licensee for the public safety broadband spectrum. As part of the Partnership, the commercial licensee will build out a nationwide, interoperable broadband network for the use of public safety. This network will facilitate effective communications among first responders not just in emergencies, but as part of cooperative communications plans that will enable first responders from different disciplines, such as police and fire departments, and jurisdictions to work together in emergency preparedness and response. Under the Partnership, the Public Safety Broadband Licensee will have priority access to the commercial spectrum in times of emergency, and the commercial licensee will have preemptible, secondary access to the public safety broadband spectrum. Many national and local public safety organizations have expressed support for a public safety/private partnership approach. Providing for shared infrastructure will help achieve significant cost efficiencies while maximizing public safety's access to interoperable broadband spectrum.

The Upper D Block commercial licensee and the Public Safety Broadband Licensee will form a Public Safety/Private Partnership to develop a shared, nationwide interoperable network for both commercial and public safety users. The terms of the Partnership will be governed both by FCC rules and by the details of the Network Sharing Agreement (NSA) to be negotiated by the Upper D Block commercial licensee and the Public Safety Broadband Licensee. The NSA is subject to FCC approval, and must contain certain provisions such as service fees and a detailed build-out schedule for the network.

DHS Office of Emergency Communications

Office of Emergency Communications (OEC) – Congress has set up the new Office of Emergency Communications at DHS. The OEC supports and promotes the ability of emergency responders and government officials to continue to communicate in the event of natural disasters, acts of terrorism, or other man-made disasters, and works to ensure, accelerate, and attain interoperable and operable emergency communications nationwide.

- New Title XVIII of the 2002 Homeland Security Act directs that OEC develop a “baseline assessment” of Federal, State, local, and tribal governments that—
 - Defines the range of capabilities needed by emergency response providers and relevant government officials to continue to communicate in the event of natural disasters, acts of terrorism, and other man-made disasters
 - Defines the range of interoperable emergency communications capabilities needed for specific events
 - Assesses the current available capabilities to meet such communications needs
 - Identifies the gap between such current capabilities and defined requirements
 - Provides a national interoperable emergency communications inventory that—
 - Identifies channels, frequencies, nomenclature, and the types of communications systems and equipment used by each Federal department and agency
 - Identifies the interoperable emergency communications systems in use by public safety agencies
- The OEC Baseline results and findings will provide valuable input into the development of the National Emergency Communications Plan (NECP), which will provide recommendations to—
 - Support and promote the ability of emergency response providers and relevant government officials to continue to communicate in the event of natural disasters, acts of terrorism, and other man made disasters; and

- Ensure, accelerate, and attain interoperable communications nationwide
- Title XVIII specifies that in developing the NECP, the OEC shall cooperate with the National Communications System (NCS) (as appropriate) and with—
 - State, local, and tribal governments
 - Federal departments and agencies
 - Emergency response providers, and
 - The Private sector

Useful References

Many of the references to useful Emergency Communications information are also included in Appendix 2 to the NCEC White Paper:

- [ANSI Homeland Security Standards Database](#)
- [ANSI Homeland Security Standards Panel](#)
- [ANSI HSSP Workshop on Emergency Communications](#)
- [APCO Project 25 Web site](#)
- CDMA Development Group ([CDG](#)) announcement regarding [use of cdma2000® technology for public safety users](#). The CDMA Development Group (CDG) announced that leading infrastructure providers, including Airvana, Alcatel-Lucent, Huawei and Nortel are offering cdma2000® 1xEV-DO Rev. A broadband equipment to support federal, state and local government public safety and first responder organizations. The first such Rev. A system is already being deployed by the National Capitals Region (NCR) in Washington, D.C., with coverage including the White House and U.S. Capitol building, to support national security, emergency response and other public safety services.
- DHS SAFECOM [Interoperability Basics](#) documents and guides.
- DHS SAFECOM [Interoperability Case Studies](#).
- “Disaster Relief: Improving Response and Long Term Recovery” White Paper and Report by the U.S. Chamber of Commerce and Booz Allen Hamilton, July 11, 2005 www.boozallen.com
- Federal Communications Commission (FCC) Report to Congress, Spectrum Requirements for Emergency Communications, December 2005. www.fcc.gov
- Federal Communications Commission (FCC), Public Safety and Homeland Security Bureau. For spectrum-related information, hot topics, Public Safety National Coordination Committee information, regulatory actions and decisions, Public Safety Wireless Advisory Committee information, national/regional plan action, radio services and licensing information, frequency coordinator information, spectrum reform, and FCC rules, visit <http://www.fcc.gov/pshs/>

- [GETS](#) Web page.
- National Consortium for Justice and Information and Statistics [links](#)
- National Institute for Urban Search and Rescue www.niusr.org
- National Institute for Standard and Technology (NIST) [Public Safety Wireless Technology Links](#)
- National Law Enforcement and Corrections Technology Center (NLECTC), a program of the [National Institute of Justice](#). "[Why Can't We Talk? When Lives Are at Stake video](#)" (NCJ 172213), call 800-248-2742. For more information on public safety radio spectrum and interoperability issues, including the AGILE program visit the NLECTC World Wide Web site at www.nlectc.org.
- National Public Safety Telecommunications Council (NPSTC). For information on NPSTC, a federation of 11 associations that acts as a resource and advocate for public safety telecommunications issues, visit www.npstc.org.
- National Security Telecommunications Advisory Committee ([NSTAC](#)) and [NSTAC Task Force on Emergency Communications and Interoperability](#).
- National Telecommunications and Information Administration (NTIA) Spectrum Management Division—[Public Safety Program Office](#), U.S. Department of Commerce. The Public Safety Program was established to coordinate the various spectrum and telecommunications-related [grants](#), activities and programs within the Federal Government as it relates to public safety.
- NTIA's Public Safety Division and the Public Safety Wireless Network Program co-sponsored a 2-day forum [Emergency Planning and Public Safety Division: Interoperability Technology Summit](#) on June 11 and 12, 2002 at The Ronald Reagan Building in Washington, DC. The Summit provided Federal and State CIOs, Congressional staffers, and local decision-makers with technology solutions for achieving interoperability among Federal/State/local public safety entities.
- National Task Force on Interoperability: "[Why Can't We Talk? Working Together To Bridge the Communications Gap To Save Lives.](#)" [Guide](#) for public safety officials. February 2003.
- [Project 25 Technology Interest Group](#)
- [Project MESA](#)
- Public Safety Wireless Network Program ([PSWN](#)), a joint program of the U.S. Departments of Justice and the Treasury. An initiative established for the planning, development, and implementation of an intergovernmental wireless network for all types of local, State, and Federal public safety agencies. PSWN is in a transitional period now due to creation of DHS and changes in funding streams. For the first time in recent memory, no future PSWN symposia are scheduled
- Satellite Industry Association (SIA) [First Responder's Guide to Satellite Communications](#). When disaster strikes, access to reliable communications is crucial to the efforts of disaster relief

operations where quick response translates into lives saved. For those times when the terrestrial communications infrastructure is damaged, destroyed or overloaded, satellite communications can provide a communications lifeline for people on the front lines of public safety and emergency preparedness. Now there is a new tool to help this crucial first responder community integrate satellite into their communications plans. The [First Responder's Guide to Satellite Communications](#) is a comprehensive overview and tutorial of satellite technology and its role in response to natural or man-made disasters.

- “Satellite Industry Response to Hurricane Katrina”, Satellite Industry Association, Fall 2005, www.sia.org
- “Special Edition on Mobile Satellite’s Role in Hurricane-Hit United States” Mobile Satellite User’s Association, Volume 14, No. 5, Oct. 2, 2005, msua@msua.org
- “[Testimony on behalf of the Satellite Industry Association](#) by Tony Trujillo, Exec. V.P. of Intelsat”, Hearing on Public Safety Communications on 9/11 to Katrina: Critical Public Policy Lessons, U.S. House of Representative, Committee on Energy and Commerce, Subcommittee on Telecommunications and the Internet, Sept. 29, 2005. [Copy to FCC Katrina Panel](#) also.
- [TIA CIP/HS and Public Safety Web site](#)
- [TIA Project 25 Web site](#)
- TIA Web site www.tiaonline.org
- "Toward a Next Generation Strategy: Learning from Katrina and Taking Advantage of New Technologies," [White Paper by Dale Hatfield and Phil Weiser](#), University of Colorado-Boulder, Prepared on behalf of Mobile Satellite Ventures.
- [2001 TIA Standards and Technology Annual Report](#). “*Emergency Responders Depend on Public Safety Radio Standards to Save Lives and Safeguard Property.*” Pages 10-15.
- “2011- What We Still Haven’t Learned” *Atlantic Monthly* January, 2005, “Why Satellite Communications Are an Essential Tool for Emergency Management and Disaster Recovery” Joint White Paper by the Futron Corporation and the Global VSAT Forum info@futron.com
- [Wireless Priority Service \(WPS\)](#) National Communications System Web page