P c Safety and E rgency Response

This Briefing Pa s a synopsis of sections as they relate rtation in Chapter 16 of the National Broadb Chapter 16 covers public safety and e response. This section also includes links to arter Public Safety".[2]

A cutting-edge y communications system uses broad ologies:

- rst responders anywhere in the natior d receive critical voice, video o save lives, reduce injuries and preve rime and terror.
- all Americans can access emergency s nation, regardless of how it is transmi
- ionize the way Americans are notified ergencies and disasters so ve information vital to their safety.
- threats to e-commerce and other Inte l applications by ensuring the the nation's broadband networks.

Broadband can 911 and emergency alert systems more capable, a better protection of lives and property. For ex h broadband, 911 call centers (also known as public wering points or PSAPs) could receive text, pictures ar om the public and relay them to first responders. Sim government could use broadband net sseminate vital information to the public du encies in multiple formats and langua , well-structured and well-protected broac works could reduce threats to Internet- lications. The proliferatio et Protocol (IP)-based communication stronger cybersecurity. Disasters and pa an lead to sudden disruptions of norm flows. As a result, broadband com ns networks must be held to high stan liab security. The re tions in this chapter are designed to r vision.

n

RECOMMEND

Promote public eless broadband communications.

- The Fec rnment should create a nationwide interoperable public safety wireless broadband communications network (public safety broadband network).
- Government should survey public safety broadband

[1] http://www.broadband.gov/download-plan/

[2] Links to IBM's Smarter Cities: Smarter Public Safety

wireless infrastructure and devices.
- Government should ensure that broadband satellite service is a part of any emergency preparedness program.
- Government must preserve broadband communications during emergencies.

Promote cybersecurity and the protection of critical broadband infrastructure.
- The Federal Communications Commission (FCC) should issue a cybersecurity roadmap.
- The FCC should expand its outage reporting requirements to broadband service providers.
- The FCC should create a voluntary cybersecurity certification regime.
- The FCC and the Department of Homeland Security (DHS) should create a cybersecurity information reporting system (CIRS).
- The FCC should expand its international participation and outreach.
- The FCC should explore network resilience and preparedness.
- The FCC and the National Communications System (NCS) should create priority network access and routing for broadband communications.
- The FCC should explore broadband communications' reliability and resiliency.

Encourage innovation in the development and deployment of Next Generation 911 (NG 911) networks and emergency alert systems.
- The National Highway Traffic Safety Administration (NHTSA) should prepare a report to identify the costs of deploying a nationwide NG 911 system and recommend that Congress consider providing public funding.
- Congress should consider enacting a federal regulatory framework.
- The FCC should address IP-based communications devices, applications and services.
- The FCC should launch comprehensive next-generation alert system inquiry.
- The Executive Branch should clarify agency roles on the implementation and maintenance of a next-generation alert and warning system.

What are your community's plans for public safety communications?

Recommendation 16.1: Create a public safety broadband network.
- Create an administrative system that ensures access to sufficient capacity on a day-to-day and emergency basis. An administrative system must ensure that users of the public safety broadband spectrum have the capacity and service they require for their network and can leverage commercial technologies to capture economies of scale and scope. There are significant benefits, including cost efficiencies and improved technological advancement, if the public safety community can increasingly use applications and devices developed for commercial wireless broadband networks. Ultimately, this system must be flexible, allowing public safety entities to forge incentive-based partnerships with commercial operators and others.

In more detail, this administrative system should include: *An opportunity to enter flexible spectrum-sharing partnerships with commercial operators.* The public safety community must be able to partner with commercial operators and others (such as systems integrators) to lower the costs of building the network and encourage its evolution. Unlike the previous approach that focused solely on the D block, an incentive-based partnership model that addresses not just the D block, but commercial wireless spectrum more broadly, will provide enhanced flexibility and the benefits of economies of scale. Such partnerships should be subject to interoperability requirements set forth by ERIC (**Emergency Response**

Interoperability Center). Public safety licensees should also be able to allow non-public safety partners to use their spectrum on a secondary basis—that can be preempted—through leasing or similar mechanisms. Partners could include critical infrastructure users such as utilities connecting to the Smart Grid. However, any revenues received by a public safety entity for such use must be used to build or improve the public safety broadband network.

Public safety access to roaming and priority access on commercial networks

- **To improve the capacity of public safety networks during emergencies, the FCC intends to begin a rulemaking to require commercial mobile radio service providers to give public safety users the ability to roam on commercial networks in 700 MHz and potentially other bands.** The rulemaking also should stipulate that, when a public safety broadband wireless network is at capacity or unavailable, authorized public safety users should get priority access on commercial networks, including all networks using the 700 MHz band and potentially other networks as well. This capacity should be available for state and local first responders as well as National Security/Emergency Preparedness (NS/EP) communications. In addition, the priority access framework should take advantage of the additional access and prioritization capabilities of 4G wireless technologies. Unlike today's circuit-switched cellular networks, 4G wireless networks can give public safety data immediate priority without waiting for commercial capacity to be freed up. Commercial operators should receive reasonable compensation for public safety priority access and roaming capabilities on their networks.

Licensing the D block for commercial use, with options for public safety partnership

- **The FCC should quickly license the D block for commercial use, while implementing several requirements for the D block licensee(s) to maximize options for partnerships with public safety.** First, the FCC should require the D block licensee(s) and the public safety broadband licensee(s) each to operate their networks using the same air interface technology standard. The emerging consensus of the public safety community and carriers is that 700 MHz networks will use the Long Term Evolution (LTE) family of standards. The FCC should consider designating this standard. A consistent air interface creates a greater likelihood of interoperability between the public safety and commercial D block networks. It will facilitate roaming between networks.

ERIC (Emergency Response Interoperability Center)

The FCC created ERIC under the umbrella of the Public Safety and Homeland Security Bureau. ERIC will develop common standards for interoperability and operating procedures to be used by the public safety entities licensed to construct, operate and use this nationwide network. ERIC will:

- Adopt technical and operational requirements and procedures to ensure a nationwide level of interoperability; this should be implemented and enforced through FCC rules, license and lease conditions and grant conditions.
- Adopt and implement other enforceable technical, interoperability and operational requirements and procedures to access, gateway functions and interfaces and interconnectivity of public safety broadband networks.
- Adopt authentication and encryption requirements for common public safety broadband applications and network use.
- Coordinate the interoperability framework of regulations, license requirements, grant conditions and technical standards with other entities (e.g., the public safety broadband licensee(s), DHS, NIST and the National Telecommunications and Information Administration).

Grants

The NBP proposes new federal grants to fund public safety broadband development. Grants to support the public safety broadband network should be distributed by a single agency to streamline operations, reduce costs and ensure that grants are made in a consistent manner. The grants should only fund projects that comply with ERIC requirements and should be made for the following four purposes:

- The construction of a public safety 700 MHz broadband network that involves partnerships and uses commercial infrastructure, the public safety infrastructure or both through incentive-based partnerships.
- The coverage of the rural areas within the network's geography.
- The hardening of the existing commercial network and new sites that operate as part of the public safety network (including covering non-recurring engineering costs for priority broadband wireless).
- The development of an inventory of deployable capability for the 700 MHz public safety band.

Using a 99% population coverage model, deployment of this network will require as much as $6.5 billion in capital expenditure in 2010 dollars over a 10-year period, which can be reduced through efficiency measures such as state and local programs and USF. Initial public funding for the capital requirement should commence in a timely manner to enable the public safety network to benefit from the planned build-outs of the private 4G wireless broadband networks, which are scheduled to begin in 2010. Congress should consider providing the bulk of these funds in the second to fifth years of the network's construction.

Fee on Broadband Use for Public Safety Network: It is essential that the United States establish a long-term, sustainable and adequate funding mechanism to help pay for the operation, maintenance and upgrade of the public safety broadband network. America's safety depends on it. Congress should consider creating such a funding mechanism in FY2011, but in any event, no later than FY2012***, Imposing a minimal public safety fee on all U.S. broadband users would be a fair, sustainable and reasonable funding mechanism. The fee should be sufficient to support the operation and evolution of the public safety broadband network.***

Promoting Cybersecurity and Protecting Critical Infrastructure

Recommendation 16.5: The FCC should issue a cybersecurity roadmap.
Admiral Mike McConnell, former Director of National Intelligence, said recently that "to the extent that the sprawling U.S. economy inhabits a common physical space, it is in our communications networks."

- Within 180 days of the release of this plan, the FCC should issue, in coordination with the Executive Branch, a roadmap to address cybersecurity. The FCC roadmap should identify the five most critical cybersecurity threats to the communications infrastructure and its end users. The roadmap should establish a two-year plan, including milestones, for the FCC to address these threats.

Recommendation 16.6: The FCC should expand its outage reporting requirements to broadband service providers.

- Today the FCC currently does not regularly collect outage information when broadband service providers experience network outages. This lack of data limits our understanding of network operations and of how to prevent future outages. The FCC should initiate a proceeding to

extend FCC Part 4 outage reporting rules to broadband Internet service providers (ISPs) and interconnected VoIP providers.

Recommendation 16.7: The FCC should create a voluntary cybersecurity certification program.

- Nearly half of all businesses in the 2009 Global State of Information Security Study reported that they are cutting budgets for information security initiatives. A 2008 Data Breach Investigations Report concluded that 87% of cyber breaches could have been avoided if reasonable security controls had been in place. The FCC should explore how to encourage voluntary efforts to improve cybersecurity.

Critical Infrastructure Survivability

Recommendation 16.10: The FCC should explore network resilience and preparedness.

- Simultaneous failure of or damage to several IP network facilities or routers could halt traffic between major metropolitan areas or between national security and public safety offices. Because many companies co locate equipment, damage to certain buildings could affect a large amount of broadband traffic, including NG 911 communications.

- This proceeding should also examine commercial networks' preparedness to withstand overloads that may occur during extraordinary events such as bioterrorism attacks or pandemics. DHS has developed pandemic preparedness best practices for network service providers, but adherence to these voluntary standards is not tracked. For example, a surge in residential broadband network use during a pandemic or other disaster could hinder network performance for critical users and applications by hindering the flow of time-sensitive medical and public health information over public networks.

Recommendation 16.11: The FCC and the National Communications System (NCS) should create priority network access and routing for broadband communications.

- Broadband users in the public safety community have no system of priority access and routing on broadband networks.

Recommendation 16.12: The FCC should explore standards for broadband communications reliability and resiliency.

- For years, communications networks were designed and deployed to achieve "carrier-class" reliability. As the communications infrastructure migrates from older technologies to broadband technology, critical communications services will be carried over a communications network that may or may not be built to these high standards. The potential decline in service reliability is a concern for critical sectors, such as energy and public safety, and for consumers in general.

Leveraging Broadband Technologies to Enhance Emergency Communications with the Public

The Move to Next Generation 911

The nation's 911 system is evolving toward supporting NG911, which will integrate the core functions and capabilities of Enhanced 911 (E911) while adding new 911 capabilities in multiple formats, such as texting, photos, video and e-mail. NG911 also will integrate entities involved in emergency response beyond the PSAP. The four fundamental purposes of NG911 are to:

- Replace the E911 system while retaining its core functions, such as automatic location information and automatic number identification.
- Add capabilities to support 911 access in multiple formats for all types of originating service providers, application developers and device manufacturers.
- Increase system flexibility, redundancy and efficiency for PSAPs and 911 governing authorities.
- Add capabilities to integrate and interoperate with entities involved in emergency response beyond the PSAP.

Broadband will make it possible for PSAPs to push and pull video, images, medical information, environmental sensor transmissions and a host of other data through shared databases and networks. This will make it easier for the public— including persons with disabilities—to access 911 services. Users will be able to transmit voice, text or images to PSAPs from a variety of broadband-capable devices.

Recommendation 16.13: The National Highway Traffic Safety Administration (NHTSA) should prepare a report to identify the costs of deploying a nationwide NG 911 System and recommend that Congress allocate public funding.

- The lack of coordinated funding is a significant roadblock for NG911 deployment. Several agencies administer existing grant and loan programs without any central coordination or uniform criteria. Moreover, limited information has been developed on the potential cost of NG911 implementation.
- Though DOT estimated in mid-2008 that the total cost of implementing and operating a nationwide NG911 system over the next 20 years would be $82 to $87 billion, the country requires a more detailed and targeted report to help Congress develop a grant program. A NHTSA analysis should determine detailed costs for specific NG911 requirements and specifications, and specify how costs would be broken out geographically or allocated among PSAPs, broadband service providers and third-party providers of NG911 services. The NHTSA report should also address the current state of NG911 readiness among PSAPs and how differences in PSAP access to broadband across the country may affect costs.

Recommendation 16.14: Congress should consider enacting of federal NG 911 regulatory framework.

- Federal and state regulations that focus on legacy 911 systems have hampered NG911 deployment. Many rules were written when the technological capabilities of NG911 did not exist. Congress should consider establishing a **federal legal and regulatory framework** for development of NG911 and the transition from legacy 911 to NG911 networks. This framework **should remove jurisdictional barriers and inconsistent legacy regulations and provide legal mechanisms** to ensure efficient and accurate transmission of 911 caller information to emergency response agencies.
- Congress should also consider steps to curtail Tribal, state and local use of 911 funds for purposes other than 911.

Recommendation 16.15: The FCC should address IP-based NG911 communications devices, applications and services.

- The FCC is considering changes to its location accuracy requirements and the possible extension of Automatic Location Identification (ALI) requirements to interconnected VoIP services. The FCC should expand this proceeding to explore how NG911 may affect location accuracy and ALI.

- The current 911 system will also need to be re-evaluated as broadband-based communications continue to proliferate. The 911 system mainly provides a voice-centric communications platform between the public and 911 operators. However, the deployment of different types of communications, devices, applications and services has meant consumers are changing their expectations about how they can access 911.

Moving Toward Next-Generation Alerting

Building on today's emergency alerting technology, FEMA has taken steps to develop an Integrated Public Alert and Warning System (IPAWS) that will lead to a next-generation public alert and warning system. The IPAWS vision is to build and maintain an effective, reliable, integrated, flexible and comprehensive system that allows Americans to receive alert and warning information through as many communication pathways as possible. But in a September 2009 report, GAO identified a number of challenges with IPAWS implementation, including some related to the inclusion of new technologies, stakeholder coordination and technical issues. ***States and localities need additional resources to upgrade their alerting operations to effectively access IPAWS.***

Links to IBM's Smarter Cities: Smarter Public Safety

http://www.youtube.com/watch?v=ibesZf_k1Uo&feature=related
Communities can increase public safety through incident management and smarter emergency systems.

http://www.youtube.com/watch?v=_a6vHAhgjW4&feature=channel_video_title
Leaders from IBM and the Center for Community Criminology and Research discuss how technology helps in crime prevention and investigation, and further establish smarter public safety that yields citizen satisfaction and economic growth.

http://www.youtube.com/watch?v=8EtH25GA_F4&feature=channel_video_title
IBM and the City of Madrid teamed up to create an innovative new response center that coordinates the resources and efforts of the police, fire, highway, hotline and ambulance units, among others. The 90-foot wall of screens displays traffic video from surveillance cameras, maps with GPS data, and the status and location of personnel. The Center was created in response to the aftermath of the terrorist train bombings on March 11, 2004, which triggered a swift, massive, but uncoordinated medical response. Radio communications were on incompatible frequencies and communication at the scene was limited to personal contact or telephone. Today, the Centre coordinates a fast, integrated response from the right team to a wide variety of emergencies.

ftp://ftp.software.ibm.com/software/solutions/pdfs/ODB-0144-01F.pdf
An innovation leader in tactics, NYPD needed to exploit its data resources more effectively to strengthen its processes. By integrating its siloed crime data systems, NYPD gets a more holistic view of information it can act on more rapidly. IBM and Business Partner Cognos created a real-time Crime Information Warehouse that makes NYPD more proactive and effective in fighting crime. Benefits include the ability to redeploy resources in response to crime patterns and trends; ability to resolve crimes and apprehend criminals more quickly.