PUBLIC SAFETY REPORT

COMMUNICATIONS SOLUTIONS FOR PUBLIC SAFETY

CONTENTS

A New View

Developing a workable next-generation network for public safety means rethinking entrenched ideas and looking toward a future roadmap.

By Dale Hatfield and Philip Weiser

The University of Colorado Law School's Silicon Flatirons Program convened a round table on public-safety communications April 11 – 12 in Washington to discuss issues facing U.S. first-responder communications and to draft a report that captured the rough consensus of the leaders who attended from academia, industry, and public safety. Participants in the round table identified shared priorities, outlined next-generation technological

solutions, and provided thoughtful analysis toward finding solutions for addressing challenges facing public safety in the near- and long-term future. The Silicon Flatirons report, which was written based on the discussion, attempts to capture the spirit and high quality of the round table's discussion. The round table, sponsored by CTIA, developed a number of conclusions, including that a progressive view must be a central feature of sound homeland-security policy going forward. Following is a summary of the report and recommendations.

The migration to next-generation networks (NGNs) represents a crucial opportunity to introduce a new paradigm where public safety is conceived of as an enterprise. Progressive public-safety agencies must adopt a broader view of communications technology, embracing the idea of a converged ecosystem. Over time, public-safety entities will need to transition away from specialized networks built solely for and operated solely by public-safety agencies. Notably, because the public-safety enterprise spans geographic jurisdictions, encompasses different agencies, and cuts across local, state, and federal governmental spheres, it's crucial that all parts of a next-generation public-safety communications system be developed in concert so that tomorrow's overall network — which will by necessity incorporate different networks and resemble a "network of networks" — is greater than the sum of its parts.

Stated simply, individual public-safety agencies will achieve greater communications capabilities if they are willing and able to work together and rely on communications technology that they may not exclusively own or control. However, this doesn't mean that one size must fit all; it's imperative that tomorrow's network accommodate tailoring to localized needs. Such tailoring, however, should be achieved within a larger interoperable and coordinated communications system. To facilitate interoperability and achieve economies of scale, networks should be operated at high levels. In short, local agencies should be empowered with the ability to use information and communications technology as needed without bearing the responsibility for running advanced networks.

General principles to guide the development of an NGN for public safety include reliability, security, openness, modularity, extensibility, and reliance on commercial, broadly supported standards.

The Turning Point

Development of an NGN for public safety presents an inflection point for first responders. Such networks should be broadband, IP based, and capable of handling voice, data, image, video, and multimedia content. By contrast, the current public-safety system, taken as a whole, is compromised by fragmented systems using disparate bands of spectrum and incompatible standards, causing both operability and interoperability problems. The piecemeal development of current incompatible systems wasn't irrational; it largely occurred in a prior technological age in which current seamless wireless capabilities were barely fathomed. Nonetheless, to properly equip the nation's first responders, communications systems must leverage 21st century technologies.

Significantly, current narrowband channels and other aspects of public-safety architecture essentially preclude existing systems from evolving into next-generation broadband networks capable of seamlessly handling voice, data, image, and video traffic on a common platform — the type of transformation already well under way in commercial cellular radio systems. Interim solutions — such as the Project 25 (P25) standard and use of gateways — help bridge interoperability deficiencies and diminish operability shortcomings. However, they suffer from notable drawbacks and aren't long-term solutions. For example, the P25 standard's narrowband technology isn't a path to supporting broadband applications and is limited in its ability to leverage commercial broadband developments. Additionally, gateway or network-based solutions, while helpful in resolving near-term interoperability problems, are hindered by drawbacks such as spectrum inefficiency and aren't ideal long-term solutions. In short, public-safety organizations have identified a pressing need for broadband capabilities, and policymakers are just beginning to develop strategies to facilitate this development.

General principles to guide the development of an NGN for public safety include reliability, security, openness, modularity, extensibility, and reliance on commercial, broadly supported standards. An NGN for public safety should benefit from the economies of scale and scope — the larger competitive ecosystem — associated with commercial systems while meeting the continuing public-safety community needs for mission-critical voice communications. It's critical that an NGN be attentive to the specialized needs of the public-safety community. And the requirements for public safety's mission-critical voice capabilities must be included in the initial specifications for a public-safety NGN to develop systems that will eventually be capable of handling all traffic on a fully converged network that captures economies of scope, improves spectrum efficiency, and reduces the need for gateways.

Public-Safety Readers Speak Out

By Sandra Wendelken

MissionCritical Communications recently surveyed its readers to determine what types of public-safety networks and technology they use. We also asked for feedback on Project 25 (P25) and interoperability issues.

The majority of survey respondents use both digital and analog networks (49 percent), but nearly as many use only analog technology (44 percent) compared with only about 8 percent of respondents who use only digital networks.

Conventional technology still rules public-safety arenas, with 46 percent of respondents using conventional networks, and 38 percent of respondents using a combination of trunked and conventional networks. About 16 percent of survey takers use only trunked networks. Most respondents (39 percent) operate on a single-agency network, while one-third use a regional system, and nearly 22 percent operate on statewide systems.

Snapshot Survey

For all the criticism often thrown at P25 from those inside and outside the industry, the public-safety communications standard fared well with respondents. Nearly 40 percent of survey takers use P25 networks. When asked how effective the standard is, the majority (52 percent) say P25 is effective for most public-safety agencies compared with 27 percent of respondents who say P25 isn't an effective standard.

Behind P25, Motorola's Astro SmartNet and SmartZone systems are used by 24 percent of survey respondents, while about 17 percent use EDACS technology from M/A-COM. iDEN networks are used by nearly 12 percent of respondents, and about 9 percent use SmarTrunk II technology from SmarTrunk Systems.

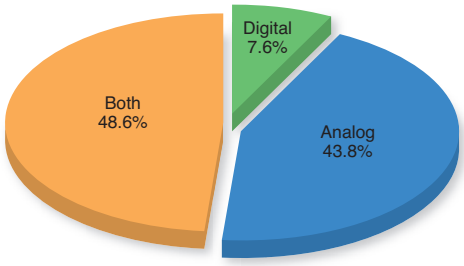
The majority of respondents do not use commercial networks, while nearly 21 percent use commercial networks for data communications. Interestingly, 15 percent of survey takers use commercial networks as their main voice-communications systems, with 14 percent of respondents using commercial networks for backup voice communications.

A majority of survey takers (57 percent) use mobile-data networks, with 16 percent using commercial EV-DO networks, and 13 percent using proprietary technologies.

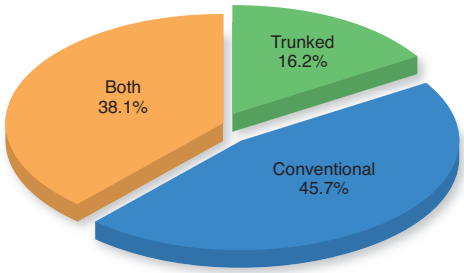
Funding, politics, and technology are the three largest challenges to interoperability among the survey respondents, with governance and standard operating procedures lagging closely behind the top three. Finding money to pay for systems also was a theme in comments from readers who took the survey. ■

Sandra Wendelken is editor of *MissionCritical Communications*. Contact her at swendelken@RRMediaGroup.com.

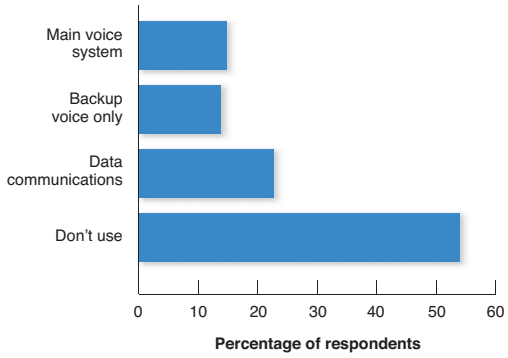
Analog over Digital



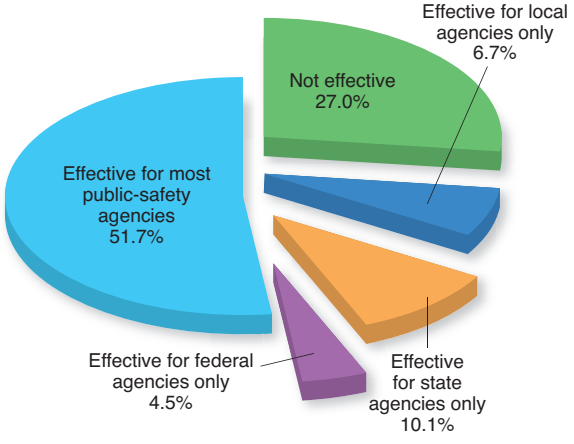
Conventional over Trunked



Commercial Network Use



Project 25



These needs include rapid call setup time and group-calling capabilities representative of modern narrowband public-safety systems, as well as other features including multiple talk groups, talk-around capabilities, multi-level priority access, pre-emption, and end-to-end encryption for privacy and security.

The Models

As public safety moves toward an NGN operated at high levels, NGN coordination models should be carefully considered and fleshed out. A public-safety NGN will increasingly migrate away from the old regime of isolated actors making autonomous communications decisions, and instead, public safety will transition to a paradigm of interagency and crossjurisdictional network coordination. Against this backdrop, two dominant NGN models have emerged: the "government as contractor" and the "public-safety spectrum licensee."

Under a government-as-contractor model, government entities contract out for the development of an NGN. Recent case studies in New York City and the Washington area's National Capital Region Interoperability Program provide real-world examples of the government-as-contractor model. Under this approach, if the government effectively defines the terms, front-end competition creates valuable efficiencies, and moreover, a governmental commitment to a period of years can help entities avoid paying all capital costs upfront. A notable challenge to this model, however, is raising the necessary funds to pay for an NGN developed by a contractor.

Meanwhile, the principal alternative NGN model — a public-safety spectrum licensee — has garnered attention in connection with a 700 MHz proposal floated by the FCC and originally proposed by Cyren Call Communications. This model involves the use of a non-profit body that possesses a license to spectrum and oversees the use of that spectrum, which may be shared with other commercial users.

Mindset Changes

An NGN must overcome three distinct cultural legacies:

- Different agencies must be willing to work together and rely on communications technology that they individually do not control. They must be open to the possibility that giving up control does not require sacrificing mission-critical applications.
- Different agencies must agree to shared governance rules that will specify how the next-generation network operates.
- Agencies must adopt a broader view of communications technology, embracing the idea of a converged ecosystem and letting go of a specialized network built solely for and operated solely by public safety.

The most critical question related to the public-safety licensee model is how the relevant governance structure would work in practice. It's important that the licensee be well positioned to ensure that the cooperating private firm meets its commitments, and consequently, an effective enforcement mechanism is particularly important.

It's possible that instead of a single top-down national NGN, there will be some form of an allied and compatible network of networks, perhaps aided by a national initiative. To that end, it's conceivable that different local, regional, and state-based next-generation projects, such as those in New York and Washington, will gravitate toward compatible standards and will be interoperable with one another. This result is unlikely, however, as past efforts at cooperation among different jurisdictions have often become mired in controversy, and thus, any such achievement will require, at a minimum, considerable national leadership to ensure standardization.

Of course, coordination strategies ultimately are part of a larger and more fundamental issue: governance. Given the numerous agencies that need to cooperate with one another, no governance system will be perfect or enjoy enthusiastic support from all stakeholders. It is clear, however, that the status quo — with a lack of effective cooperation among agencies — is a recipe for perpetuating the current shortcomings. To date, neither FCC regulations nor Department of Homeland Security (DHS) grants have galvanized strategic planning and coordination at the regional or state levels to the degree necessary to transform the autonomous and fragmented culture of public-safety communications. In short, different local agencies will have to compromise and give up some control over what communications systems they use to enable effective coordination with one another. Without coordination, different agencies won't be able to develop and abide by shared governance rules that specify how the NGN will operate — including what services will be available to whom and under what circumstances.

The Transition

In many respects, the near term presents the most challenging public-safety funding demands. Policymakers must make do with legacy systems and facilitate the development of an NGN system at the same time. Given public-sector funding cycles and constraints, existing public-safety narrowband systems will remain in place for years to come, and backward compatibility of any NGN will remain critical to ensure interoperability. Ultimately, once a next-generation system is well proven and adopted by public-safety agencies, there may be an opportunity for those agencies to abandon their legacy equipment, and in some cases, traditional spectrum allocations. But such a day is far in the future and uncertain. In the meantime, policymakers face the dual challenges of facilitating the development of the best possible technologies to work in conjunction with existing systems, as well as laying the groundwork for a next-generation architecture.

During the transition to a public-safety NGN, perfection shouldn't be

the enemy of the good. Progress toward an NGN must be cognizant of the impracticality of building a network with sufficient capacity to handle all communications needs — essential and nonessential — in times of emergency. Accordingly, priority schemes and other methods of shedding nonessential traffic will remain critical. Moreover, obtaining the last few percentage points of geographic and in-building coverage becomes prohibitively expensive in any radio-based system designed to cover a wide geographic area, and at some point, cost constraints must be acknowledged. For example, the cost to extend coverage into the third sub-basement of a major bank building may exceed public-safety benefits.

Choices between cost and coverage aren't easy ones. In cases where coverage or capacity is sacrificed, the ability of public-safety agencies to protect the public will be hampered. Such choices must be made based on reasonable cost-benefit tradeoffs. Thus, the touchstone for an NGN shouldn't be whether such systems are impervious to defect; it should be whether an NGN will deliver significantly improved and cost-effective capabilities to first responders over existing networks.

Ultimately, for America's public-safety agencies, the decision to invest in state-of-the art information and communications technology is long overdue. The first step in doing so, however, is for policymakers to realize this investment is as critical to the success of these agencies as providing them with effective equipment to protect our citizenry and respond to emergency situations across a range of life-and-death situations. ■

Dale N. Hatfield is an independent telecommunications consultant and adjunct professor at the University of Colorado at Boulder and formerly chief of the Office of Engineering and Technology at the FCC. He is an editorial advisor to *MissionCritical Communications*. Contact him at dale.hatfield@ieee.org. The full report is available at www.silicon-flatirons.org

Professor Philip J. Weiser established the Silicon Flatirons Telecommunications Program at the University of Colorado Law School. Weiser writes and teaches in the areas of telecommunications and information policy. Weiser previously served as senior counsel to the assistant attorney general in charge of the antitrust division at the U.S. Department of Justice. Weiser recently testified on public-safety communications before the Senate Commerce Committee. Contact him at phil.weiser@colorado.edu.