UTC
UTILITIES TELECOM COUNCIL
The Telecommunications and Information Technology Association for Utilities, Pipelines, And Other Critical Infrastructure Companies

Brett Kilbourne
Deputy General Counsel

Direct Line: 202.833.6807
E-mail: brett.kilbourne@utc.org

October 12, 2011

Dereck Orr
Office of Law Enforcement Standards
U.S. Department of Commerce
National Institute of Standards and Technology
325 Broadway
Boulder, Colorado 80305

Re: Soliciting Input on Research and Development Priorities for Desirable Features of a Nationwide Public Safety Broadband Network

Dear Mr. Orr:

Thank you for the opportunity to comment to NIST for consideration regarding research and development priorities for the President's Wireless Innovation (WIN) Fund to drive innovation of next-generation network technologies for a new nationwide public safety broadband network.[1] UTC urges NIST to consider issues regarding compatibility with utility infrastructure, as well as commercial infrastructure.[2]

Utilities have many of the same communications needs as public safety, including resiliency, reliability and availability, and security. Moreover, utilities have partnered with public safety to build, operate and maintain state and local public safety/public service shared systems across the country, including in Colorado, Georgia, Illinois, Nebraska, Nevada, North Carolina, Ohio, Pennsylvania and South Carolina.[3] Currently, there are two states (Nevada and Michigan) that have filed waiver requests with the FCC for authority to construct and operate a statewide 700 MHz public safety broadband network that would be shared with utilities.[4] These waiver requests reflect the reality that utilities and

[1] *See* Notice and Request for Comment: Soliciting Input on Research and Development Priorities for Desirable Features of a Nationwide Public Safety Broadband Network, Docket No. 110727437-1433-01, 76 Fed. Reg. 56,165, Sept. 12, 2011 ("Notice").

[2] *See* Notice at 56166 (inviting comment on various issues to "ensure affordability/commercial alignment," including "Compatibility with Commercial Infrastructure.")

[3] *See* Comments of the Utilities Telecom Council in response to the FCC's Third Report and Order and Fourth Further Notice of Proposed Rulemaking, WT Docket No. 06-150; PS Docket No. 06-229, 26 FCC Rcd. 733 (2011) at 2 (filed Apr. 11, 2011).

[4] *See* Las Vegas Metropolitan Police Department, Washoe County Sheriff's Department, the Washoe Regional Communications System, the Nevada Department of Transportation, and NV Energy, representing the State of Nevada 700 MHz Broadband Wireless Network (SONNet) Request for Waiver – Expedited Action Requested, WT Docket No. 06-229 (filed May 13, 2010); *and* Request by the State of Michigan for a Waiver of the Commission's

public safety make good partners, given their similar communications needs and the resources they can contribute towards sharing costs. The FCC has recognized this, which is why it recommended in its National Broadband Plan that Congress amend the Communications Act to promote sharing 700 MHz public safety broadband networks with utilities.[5] Congress is currently considering legislation that would do just that,[6] and the FCC has a rulemaking proceeding that considers technical interoperability issues, including sharing the 700 MHz public safety broadband network with utilities.[7]

Utilities design, build and maintain their communications networks to high standards for resiliency, reliability and availability and security. For example, utilities require uninterrupted back-up power (e.g. batteries and generators) at each site to ensure reliability of communications for extended periods (e.g. 72 hours or more). They also design their systems with redundant/diverse backhaul to ensure that communications are maintained, even if one part of the network goes down. Finally, they require coverage all across their service territories, even into remote areas. These attributes all contributed to the reliability and resiliency of utility networks in the aftermath of Hurricane Katrina and other hurricanes that struck the southeast in 2005. They were the only communications networks – public or private – that continued to operate in the affected areas during and after the hurricanes.[8]

Rules to Allow Establishment of a 700 MHz Interoperable Public Safety Broadband Network in the State, WT Docket No. 06-229 (filed Sept. 16, 2011).

[5] Connecting America: The National Broadband Plan, p. 270 at http://www.broadband.gov/plan/12-energy-and-the-environment/#r12-4
(stating that "[t]he wide-area network requirements of utilities are very similar to those of public safety agencies. Both require near universal coverage and a resilient and redundant network, especially during emergencies.")

[6] *See e.g.* "Public Safety Spectrum and Wireless Innovation Act," S. 3756, 111th Cong. 2d. Sess. at Sec. 104.

[7] *See* Service Rules for the 698-746, 747-762 and 777-792 MHz Bands, ; Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band, Third Report and Order and Fourth Further Notice of Proposed Rulemaking, WT Docket No. 06-150; PS Docket No. 06-229, 26 FCC Rcd. 733 (2011)(hereinafter Fourth Further Notice). UTC's comments also briefly address the FCC's Public Notice inviting comment on the request for declaratory ruling by the City of Charlotte in this proceeding. See Public Safety and Homeland Security Bureau Seeks Comment on Petition for Declaratory Ruling Asking to Clarify the Scope of Section 337 Regarding Use by State or Local Government Entities of the 700 MHz Public Safety Broadband Spectrum, Public Notice, PS Docket No. 06-229, 2011 WL 1044284.

[8] *See e.g.* Utility communications networks proved their survivability in the aftermath of Hurricane Katrina and other Gulf Coast hurricanes during 2005. While commercial systems were out for a week or more after the hurricane, SouthernLINC Wireless (a subsidiary of Southern Company) reported that 98% of its cell sites were back in operation within three days. It also reported that SouthernLINC wireless "contributed greatly to public safety and restoration of public services," including electric service in the affected states. *See* generally Letter from Jeffrey L. Sheldon, Counsel to Southern Company, to Nick Sinai, Energy and Environment Director at FCC, FCC Docket No. 09-51 (filed Feb. 5, 2010). *See* also Final Report of the Commission's Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks ("Katrina Panel Final Report") at http://www.fcc.gov/pshs/docs/advisory/hkip/karrp.pdf (stating that "Mississippi Power relied on its only viable form of communication – its internal system Southern Linc Wireless. This system was designed with considerable redundancy and proved reliable despite suffering catastrophic damage. Within three days, the system was functioning at nearly 100 percent.") *And see* "Hurricanes of 2005: Performance of Gulf Coast Critical Infrastructure Communications Networks," United Telecom Council, November 2005 at http://www.utc.org/fileshare/files/34/Research/white_papers/2005_-_UTC_-_HURRICANES_OF_2005_PERFORMANCE_OF_GULF_COAST_CIC_NE.

The same cannot be said for commercial communications networks. For example, commercial wireless providers successfully challenged an FCC rule that would have required a minimum of eight hours of battery back-up at each cell site. They fought this requirement for a variety of reasons, including economic, technical and political reasons. Presumably, they have yet to implement true uninterruptible backup power that is available for extended periods of time. Similarly, it is not at all clear that commercial networks have redundant/diverse routing to ensure reliable communications when a line is cut or some part of the network goes down.[9] In fact, there are numerous examples where system outages were experienced on commercial networks due to such backhaul problems. Finally, there are many areas that are not served by commercial service providers, but of course would need to be in order to support public safety.

These are just some of the reasons why we believe that NIST should be considering alignment with utilities, as well as commercial service providers. There are real advantages to public safety by sharing with utilities. Public safety could leverage utility infrastructure and would need interoperable communications with utilities during emergencies. Utilities have extensive infrastructure and they have rights of ways that could be used to construct new facilities, which could be particularly useful for the 700 MHz public safety broadband network in insular and remote areas that are not currently served or are underserved by commercial service providers. Public safety also needs to effectively coordinate with utilities during emergencies, including localized emergencies (e.g. turning off the gas in a burning building) and widespread emergencies (e.g. downed powerlines in the aftermath of a storm). Sharing the 700 MHz public safety broadband network would promote interoperability with utilities because users would share the same spectrum.

Utilities have an interest in some of the detailed issues that NIST is considering in this proceeding, including priority access, quality of service and strong dynamic access control. Utilities need to have priority access along with public safety during emergencies; they cannot afford to have mission critical communications subject to preemption. UTC believes that LTE technologies provide multiple levels of priority access, which should be able to accommodate the communications needs of both public safety and utilities. Having said that, utilities would have an interest in NIST efforts with regard to research and development on priority access. Similarly, utilities need communications that have high quality performance for critical applications; and utilities would also have an interest in NIST efforts with regard to research and development on quality of service. Finally, utilities need networks that are secure; and they would have an interest in NIST efforts with regard to research and development with regard to in-bound and out-bound traffic and authentication/verification of devices on the network.

UTC is concerned that NIST may be overlooking utilities, which could unintentionally create barriers to public safety partnerships with utilities. There may be unique issues associated with sharing with utilities, including multi-modality, scalability, power awareness, standardized common interfaces and uniform universal access. While NIST is addressing those issues with respect to public safety as part of this proceeding, if technology solutions are developed that do not address issues that are unique to utilities, those solutions may discourage or prevent utilities from effectively sharing the network with public safety. Conversely, that would needlessly frustrate the ability of public safety and policymakers to

[9] *See In the Matter of Reliability and Continuity of Communications Networks, Including Broadband Technologies; Effects on Broadband Communications Networks of Damage or Failure of Network Equipment of Severe Overload; Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks*, Notice of Inquiry, PS Docket Nos. 11-60 and 10-92, EB Docket No. 06-119, FCC 11-55 at ¶40 (April 7, 2011) (stating that "the access portions of most networks generally contain single points of failure.")

take advantage of the aforementioned benefits that could be gained from sharing the network with utilities.

For all of these reasons, UTC encourages NIST to consider issues related to sharing the 700 MHz public safety broadband network with utilities, as well as commercial service providers. UTC thanks the NIST for the opportunity to comment in this proceeding and looks forward to working with NIST on this matter in the future.

If there are any questions concerning this matter, please let me know.

Very truly yours,

Brett Kilbourne

Brett Kilbourne
Director of Regulatory Services and Deputy General Counsel

Mike Oldak
Vice President & General Counsel

Utilities Telecom Council
1129 20th Street, NW
Suite 350
Washington, DC 20036