



## IP&P25 Standards Promote Interoperability

*Efforts to create standards related to interoperability need to be cast in the context of an ever-changing reference, rather than as a single point forever cast in stone. Standards, like the technologies on which they are based, must evolve over time or they will stagnate. An initial standard specification may be completed, but an evolving standards process is never complete.*

A standards document serves as a reference tool to describe how technology should function or how an interface should work. For example, it may explain how new technology should interface with older standards-based technology (backwards compatibility), or it can provide a vendor with a way to determine if older standards-based technology must be changed to meet the latest standard. A standard can also assist potential manufacturers in identifying intellectual property associated with a given standard.

Verifying compliance with a standard can be as simple as a vendor stating “yes our technology is compliant with standard X” during a procurement process or as complex as proving compliance as part of a comprehensive testing and acceptance regimen. A standard provides the end user, possibly a procurement officer, and the potential vendor community with a common target and a language to describe that target. If a standard is not thoroughly understood and interpreted in a consistent manner, problems will be created.

Discussed here are two important interoperability standards: Internet Protocol (IP) and Project 25 (P25).

### Internet Protocol Standards

Internet protocol has become a universal technological base that affects almost every aspect of everyone’s personal and professional lives. Its many applications (such as data exchange, data and network interoperability, and wireless data) all play important roles in the overall context of public safety communications. However, even as new IP-based tools begin to resolve ongoing voice interoperability issues associated with proprietary

and incompatible multivendor public safety land mobile radio systems, a lack of IP standards may mean that yet another layer of incompatible technology is being added to the mix.

“Without an agreed-upon public safety VoIP [Voice over Internet Protocol] standard, law enforcement and public safety may become entrenched in a procurement environment dominated by incompatible, single-vendor, proprietary VoIP technology,” says Phil Harris, a contract senior communications engineer supporting the Office of Justice Programs’ National Institute of Justice (NIJ) Communications Technology (CommTech) program via the National Law Enforcement and Corrections Technology Center (NLECTC)–Northeast and the Communications Technologies Center of Excellence. He explains that the public safety community needs to be aware that suppliers can claim their VoIP technology is “standards based,” even if a product is entirely proprietary and therefore noninteroperable. In fact, any two competing products based entirely on “open and nonproprietary” IP standards will most likely be noninteroperable at the VoIP level because of manufacturers’ design choices, whether intentional or unintentional.

In an attempt to help resolve these types of fundamental issues, a government/industry working group has created an interim multivendor standard specification that can be used to establish a minimum basis for interoperability between VoIP bridging/interconnect devices. An industry/government/public safety consensus has been reached on this profile, which will serve as a baseline foundation for subsequent revisions (now underway) to improve and build on this initial effort.

“These interim profiles allow agencies to expect minimum levels of interoperability and may lead to multivendor product sourcing. They also can provide a baseline against which compliance might be made mandatory if public funding is used to purchase VoIP interoperability technology,” Harris says

This effort has been facilitated by the U.S. Department of Homeland Security (DHS) and the National Institute of Standards and Technology (NIST), with support from the U.S. Department of Commerce Institute for Telecommunications Sciences in Boulder, Colorado. Support from many industry participants has also been fundamental to its development; NIJ technical representatives regularly attend ongoing roundtable meetings on behalf of the NIJ CommTech program.

The Bridging Systems Interface (BSI) VoIP Interface Profile is based on a collection of open standards that have been identified and adopted through the consensus process. Each must be implemented in specific agreed-upon ways to facilitate and ensure multivendor interoperability between VoIP devices. This effort will eliminate, or at least minimize, potential layers of noninteroperable technology used in critical public safety applications, Harris says.

For more information, read the following documents:

- *Voice over Internet Protocol*, NIJ In Short, (<http://www.ncjrs.gov/pdffiles1/nij/217864.pdf>).
- *Telephony Implications of Voice over Internet Protocol*, NIJ In Short, (<http://www.ncjrs.gov/pdffiles1/nij/212976.pdf>).
- *Interoperability Gateways/Interconnects*, NIJ In Short, (<http://www.ncjrs.gov/pdffiles1/nij/217105.pdf>).
- *Roundtable on Public Safety Interoperability and Voice over Internet Protocol (VoIP)* (2006 and 2007 reports), (<http://www.safecomprogram.gov/NR/rdonlyres/7991A608-54A9-45A2-B6B2-2033E849BC14/0/VoIPReportfinal.pdf> and <http://www.safecomprogram.gov/NR/rdonlyres/F5097180-FD4C-463A-8050F24489853ED7/0/2ndRoundtableonPublicSafetyInteroperabilityandVoIPmeetingreport.pdf>).

For an example of VOIP in action, see “First Step to Interoperability: Cooperation,” *TechBeat* Spring 2008, at [www.justnet.org/techbeat/spring2008/](http://www.justnet.org/techbeat/spring2008/).

## P25 Compliance Assessment Program

P25 defines a suite of standards for public safety digital wireless radio communications systems to allow multiple vendors to supply products and services that will interoperate with each other.

In partnership with DHS’s Project SAFECOM and with support from NIJ’s CommTech program, the NIST Office of Law Enforcement Standards (OLES) began to develop the P25 Compliance Assessment Program in 2005. The program’s central purpose is to help emergency response officials, including law enforcement, make informed purchasing decisions. By consulting a list published on the Responder Knowledge Base ([www.rkb.us](http://www.rkb.us)),

officials will know which products have passed an established testing protocol developed under NIST oversight.

The program has three parts: a supplier declaration of compliance (SDoC), a summary test report, and a records and inspection provision. The SDoC is a formal manufacturer declaration of product compliance that provides details about product configuration and lists the types of tests applied to the product and test results, and also includes the signature of a responsible company official. The summary test report contains more details about the tests in a uniform, easy-to-review format. Finally, manufacturers are required to maintain all records of the test results, which are open to inspection by NIST representatives. Achieving the compliance assessment vision in full will take years, but NIST expects to begin implementing aspects of the program in fall 2008.

The P25 Compliance Assessment Program allows manufacturers to develop their own laboratory compliance programs, thus avoiding the need to train employees of outside laboratories. Throughout the early stages of the Compliance Assessment Program, NIST and vendors expect there to be growing pains. From time to time, both standards and procedures will be modified to resolve problems stemming from inconsistent interpretations.

“Radio systems of the past were primarily hardware-only products, but systems today depend on both hardware and software components. Consequently, legacy equipment and software upgrades, which can cause problems for smoothly functioning interoperable communications systems if not perfectly compatible with all equipment in the system, will pose a continuing challenge,” says Dereck Orr, NIST program manager for public safety communication standards. “To cope with the inevitable growing pains, NIST will try to get feedback from industry representatives and others and use it to sharpen both testing procedures and the standards themselves.”

Orr continues that participation by manufacturers is strictly voluntary: “They may develop, market, and sell P25 products without participating in the compliance program, which is similar to NIJ’s well-known body armor testing compliance program. However, DHS will restrict, aside from a few special considerations, its grants for purchasing equipment to products that appear on its published list. Manufacturers’ most detailed test reports and anything proprietary may remain confidential; only facts and data documenting compliance must be released.”

Project 25 was launched in 1989 to develop standards that define how digital land mobile radio systems should operate and how key system interface standards would allow radios and other components to interoperate regardless of manufacturer. The ultimate goal of P25 is to

specify formal standards for eight interfaces between the various components of a land mobile radio system:

- Common air interface.
- Inter-RF subsystem interface.
- Fixed station subsystem interface.
- Console sub-system interface.
- Network management interface.
- Data network interface.
- Subscriber data peripheral interface.
- Telephone interconnect interface.

## For More Information

*For more information, visit the “Project 25 CAP” section of the SAFECOM website: <http://www.safecomprogram.gov/SAFECOM/currentprojects/project25cap/project25cap.htm/>.*

## The National Law Enforcement and Corrections Technology Center System Your Technology Partner

[www.justnet.org](http://www.justnet.org)  
800-248-2742



This article was reprinted from the Fall 2008 edition of *TechBeat*, the award-winning quarterly newsmagazine of the National Law Enforcement and Corrections Technology Center System, a program of the National Institute of Justice under Cooperative Agreement #2005-MU-CX-K077, awarded by the U.S. Department of Justice.

Analyses of test results do not represent product approval or endorsement by the National Institute of Justice, U.S. Department of Justice; the National Institute of Standards and Technology, U.S. Department of Commerce; or Lockheed Martin. Points of view or opinions contained within this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

The National Institute of Justice is a component of the Office of Justice Programs, which also includes the Bureau of Justice Assistance; the Bureau of Justice Statistics; the Community Capacity Development Office; the Office for Victims of Crime; the Office of Juvenile Justice and Delinquency Prevention; and the Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking (SMART).