Department of Justice

STATEMENT

OF

DR. JOHN S. MORGAN
ASSISTANT DIRECTOR FOR SCIENCE AND TECHNOLOGY
NATIONAL INSTITUTE OF JUSTICE
OFFICE OF JUSTICE PROGRAMS
UNITED STATES DEPARTMENT OF JUSTICE

BEFORE THE

COMMITTEE ON HOMELAND SECURITY
SUBCOMMITTEE ON EMERGENCY PREPAREDNESS,
SCIENCE, AND TECHNOLOGY
UNITED STATES HOUSE OF REPRESENTATIVES

CONCERNING

"THE STATE OF INTEROPERABILITY:
PERSPECTIVES ON FEDERAL COORDINATION OF
GRANTS, STANDARDS, AND TECHNOLOGY"

PRESENTED ON

APRIL 25, 2006

House Committee on Homeland Security

Subcommittee on Emergency Preparedness, Science, and Technology

Testimony of Dr. John S. Morgan
Assistant Director for Science and Technology

National Institute of Justice
Office of Justice Programs
U.S. Department of Justice
April 25, 2006

Good afternoon Chairman Reichert, Mr. Pascrell, members of the Subcommittee. I am pleased to appear before you today on behalf of the Office of Justice Programs' National Institute of Justice (NIJ) to speak to you on the issue of public safety communications interoperability. I will address communications interoperability needs of state and local law enforcement and public safety, especially with respect to emerging technology and the need for standards.

Congress created NIJ in 1968 as the research, development and evaluation arm of the U.S. Department of Justice (DOJ). Its mission is to advance scientific research, development, and evaluation to enhance the administration of justice and public safety. NIJ's primary focus is on state and local criminal justice agencies, which are responsible for over 95 percent of the adjudication of crime in the United States. NIJ is the only federal agency dedicated to improving the effectiveness of criminal justice through scientific research. NIJ is committed to the scientific process of open competition, peer-review, published reports and archived data.

NIJ's Office of Science & Technology (OS&T) was established in 1992 to execute the agency's technology research and development program. This program includes: technology research and development; establishment and maintenance of performance standards for test and evaluation of technologies and equipment; and establishment and maintenance of the National Law Enforcement and Corrections Technology Center (NLECTC) system. The NLECTC system supports NIJ through development of technology requirements, test and evaluation, and providing technology assistance to state and local agencies through 10 technology assistance and specialty centers across the United States.

Although OS&T has been in operation for more than a decade, Congress officially recognized the office in Title II of the Homeland Security Act of 2002 (HSA). Through that legislation, Congress assigned several critical responsibilities to NIJ, including:

- To establish and maintain advisory groups to assess the technology needs of federal, state and local criminal justice agencies;

- To establish and maintain performance standards, test and evaluate law enforcement technology and equipment, and establish programs to certify, validate and mark technologies and equipment conforming to these standards;

- To take the lead in establishing a coordinated federal approach to issues relating to criminal justice technology; and

- To administer a program of research, development, testing, and demonstration to improve the interoperability of voice and data public safety communications.

NIJ has extensive experience in addressing public safety communications issues. Through its Communications Technology portfolio (CommTech), NIJ pursues both short- and long-term interoperability solutions involving wireless telecommunications and information technology. NIJ's work in this area includes:

- Research and development of technology for wireless interoperability;

- Test and evaluation of current products;

- Standards development for wireless interoperability;

- Pilot demonstrations on cutting edge technology; and

- Technology assistance to state and local agencies.

The CommTech research and development efforts are concentrated on Software Defined Radio (SDR), cognitive radio, Voice-over-Internet Protocol (VOIP), Advanced Wireless Voice and Data, and in-building location and communication technologies. As in all of its technology portfolios, NIJ maintains a practitioner-based Technology Working Group (TWG) for the CommTech portfolio comprised of state and local practitioners who offer advice on technology requirements and program direction. NIJ's CommTech investments are based on the specific needs identified to us by this TWG. NIJ also coordinates its program with all the federal agencies involved in public safety communications interoperability, including SAFECOM and the Office of Grants and Training in the Department of Homeland Security, the National Institute of Standards and Technology within the Department of Commerce, and the Office of Community-Oriented Policing Services within the Department of Justice.

These front line practitioners have identified standards development and compliance assurance as among the priorities in this area. Only a very small number of standards exist to ensure that radio systems are interoperable across jurisdictional and agency boundaries. In addition, there is no compliance testing program to ensure that systems

conform to the few standards that do exist. Compliance testing is an integral component of any standards development effort to ensure that fielded systems meet the requirements of standards.

While federal assistance programs for interoperability already include technical assistance for state and local agencies, more independent evaluations of the outcomes would be advisable. Evaluations should focus on actual compliance with standards, assessment of the fielded systems against the SAFECOM *Statement of Requirements (SoR) for Public Safety Wireless Communications and Interoperability*, and the improvements in operability and interoperability those systems produce. Such evaluations would also include fundamental examination of public safety benefits, such as improvements in response to critical incidents. Federal assistance programs in interoperability thus far have lacked such independent evaluation, therefore there is insufficient data on the impact, whether positive or negative. NIJ has a close working relationship with SAFECOM and has played a primary role in the initial development of the SoR and in its ongoing review.

The Role of Technology Development

Developing a comprehensive suite of standards and effective policy coordination are critical to addressing the issues of public safety communications interoperability and operability; but developing new technology is also vital. NIJ believes the issues of operability and interoperability are inextricably linked. Operability means that two individuals from the same agency can talk with each other. Operability deals with issues such as equipment availability, bandwidth and spectrum allocation issues for voice and data, interoperability between vendors and technology, standards, command and control, and federal, state, and local coordination. Interoperability occurs when two (or more) individuals from different public safety agencies communicate with each other. Without operability, interoperability is irrelevant. Focusing solely on interoperability will not allow the practitioner to communicate or access information effectively.

Although technology development alone will not solve all communications problems, it can provide important solutions that enable public safety to access the revolution in wireless communications underway in the commercial market. For this reason, NIJ has made significant investments in new technologies such as SDR, cognitive radio, and satellite communications for rural agencies. Such technologies should enable public safety practitioners to "roam" freely just as cell phone users do and maximize the potential of the limited radio frequency spectrum made available to the public safety community. Of course, this can take place only when standards are in place to ensure that systems will be compatible with each other through advanced technology. Any federal investment in communications should recognize the need to develop technology solutions that enable improved operability and interoperability. Cognitive radio and SDR may enable first responders to communicate seamlessly at critical incidents in the future.

A SDR radio is one where frequency range, modulation or maximum output power can be altered by making a change in software without making any changes to hardware

components that affect the radio frequency emissions. SDR may provide an efficient and comparatively inexpensive solution to the problem of building multi-mode, multi-band, multi-functional wireless devices that can be easily enhanced. As such, SDR can be considered an enabling technology that is applicable across a wide range of areas within the wireless industry, not just public safety.

Through CommTech, NIJ is funding the Public Safety Special Interest Group (PS SIG) within the SDR Forum. The goals of the PS SIG are to raise awareness of SDR, to publicize the activities of the Forum in addressing issues confronting public safety, and to increase participation of the public safety community in the SDR Forum. One of the Forum's more important undertakings is a study to assess the potential of, and issues associated with, SDR technology for the public safety community, with emphasis on disaster response. The report was approved by the SDR Forum membership this month (April 2006).

One specific SDR development example is the Dynamic Open Architecture Radio System (DOARS). DOARS is a collaboration with the U.S. Navy's Space and Naval Warfare System Center-Charleston. The project heavily leverages work in SDR projects within the Department of Defense, and seeks to create an affordable, user-friendly PC-based "universal radio" for public safety agencies.

A cognitive radio is a step beyond SDR. Whereas an SDR requires human programming, a cognitive radio will have the ability to adapt its behavior based on external factors without human intervention. A cognitive radio can alter its transmitter parameters based on interaction with the environment in which it operates, i.e., it senses what systems a radio can connect to and connects to them. This interaction may involve active negotiation or communications by the device with other devices or passive sensing and decision-making within the radios. A cognitive radio may be able to change its operating frequency to optimize use, sense signals from other nearby transmitters in an effort to choose an optimum operating environment, modify transmission characteristics, waveforms, and transmitter power to allow greater sharing of spectrum, select operating parameters based on what power and frequency are allowed at its current location, and implement "device-negotiated" sharing of spectrum under the terms of a prearranged agreement between a licensee and a third party. Cognitive radios may eventually enable parties to negotiate for spectrum use on a real-time basis, without the need for prior agreements between all parties. Of course, this will be important to both commercial and public safety customers who have limited amounts of radio spectrum available.

NIJ is funding Virginia Polytechnic Institute and State University to build a prototype cognitive radio that can recognize and interoperate with commonly used public safety waveform standards. This work leverages National Science Foundation investments to develop and test cognitive radio techniques for commercial applications.

Spectrum Allocation

Spectrum allocation is a major requirement for the effective deployment of interoperable and operable communications systems. One approach to dealing with this difficulty has been to increase the spectrum available to public safety agencies. Recent legislation that sets a date certain for the digital television transition will facilitate the reclamation of valuable spectrum resources for public safety use. This spectrum is anticipated to enable greater interoperability among public safety agencies. Another approach, which is being pursued by NIJ, is to develop technology that will enable public safety agencies to better use the limited spectrum allocated to them. NIJ is funding multiple efforts to develop such technologies that would be of use to state and local agencies receiving Federal grant funds.

 In the current fiscal year 2006 solicitation cycle, NIJ is looking to fund technologies that will utilize the newly allocated public safety bands more efficiently. This includes technologies that involve mesh, or ad-hoc, networking that operate in the 4.9 GHz band and, in the future, the 700 MHz band. We believe these efforts will allow more effective and productive use of existing bands and quicker identification of additional bands if needed to meet national objectives for our first responders.

The Current Status of Standards

It cannot be over emphasized that developing standards is vital to dealing with the issue of public safety interoperability. Long before September 11, 2001, NIJ recognized the importance of interoperability standards for the public safety community. NIJ, through CommTech, is deeply involved in development of the APCO (Association of Public-Safety Communications Officials - International, Inc.) -25, or Project-25 (P-25) standard. This initiative is an industry-wide effort to set voluntary standards for digital two-way radio technology for public safety organizations. In the early 1990s, the P-25 Steering Committee approved the very first public safety, user-driven Statement of Requirements (SoR) with the support of NIJ's CommTech Program.

NIJ funds the chairmanship of the P-25 standard steering committee, a public standards committee under the Telecommunications Industry Association, and the travel costs of some of the public safety agency representatives who participate in the process, thus helping to ensure objectivity and representativeness in the standards process. While these costs are small, less than $250,000 per year, they have provided both the impetus and the core element of a truly user-driven standards process. Within P-25, the steering committee and its user groups determine the user requirements, the standards that are acceptable, and the priority of developing those standards. Through that funding, we have leveraged the extensive economic resource of the major public safety telecommunications industry in a cooperative and consolidated effort to improve competition, provide interoperability, and ensure a transparent and achievable migration path.

Since P-25's inception, the P-25 steering committee and its partners in the Telecommunications Industry Association (TIA) have completed over 34 technology standards that will provide one of the three primary legs in our long-term efforts to create public safety interoperability. Long-term planning and interagency cooperation will also be necessary to implement interoperable communications systems across the nation.

Although significant progress has been made, there are a number of standards that need to be developed. These include:

- Inter-Sub-System Interface (ISSI) which allows a mobile from one system to transparently roam into another compatible system and have complete communication.

- Enhancement to the Fixed Station Interface to ensure easier and more complete console access.

- Enhancement of the Consol Interface Standard to ensure greater transparency.

- Completion of the Network Management standard interface.

- Enhancement of data interface to ensure transparent system-to-system data transport on a more ubiquitous bases.

- Enhancement of mobility to improve upon ease of access during roaming.

- Telephone Interconnect – ISSI compatible

A multitude of other conformance and performance standards are also needed, including interface standards for such things as global position systems or other user requirements as they arise. A total of as many as 90 standards are anticipated. The new standards that are required will be much more abbreviated than the current 34 since they will be based on many of the original standards and modified to fit the need of the next technology platform. Of course, all these new technologies and associated standards must be compatible with existing systems and standards. Public safety agencies do not have the resources to replace entire systems every few years. Even beyond these standards, there is a complete suite of needed standards that relate to spectrum efficiency. Finally, there is work continuing on broad-band data and 4.9 GHz data standards to allow the transport of high-speed wireless data among field radios and to and from major Public Safety Answering Points or Incident Management Centers. In short, there is a great deal of work that needs to be done to address standards for public safety communications.

Testing and validation of P-25 compliant technology is necessary to ensure the equipment being sold is interoperable at all levels. While there is significant compliance at the level of common-air-interface, there have been problems with the interoperability of features and functions. The P-25 steering committee, its user groups, TIA and its members, with the support of NIJ, have been aggressively working with the Department of Commerce's

National Institute of Standards and Technology's Office of Law Enforcement Standards, the Institute for Telecommunications Sciences, and SAFECOM, to develop a coordinated solution. In particular, the National Institute of Standards and Technology has made significant progress in the development of critically important compliance testing programs to implement standards in practice and provide public safety practitioners with performance assurance independent of manufacturer claims.

The long term goal of P-25 is seamless public safety communications interoperability and telecommunications transparency. Achieving that goal is dependent upon leadership, adequate funding and sound planning at all levels of government.

While the P-25 Steering Committee continues to meet and the standards continue to evolve, public safety practitioners continue to purchase communications systems. Because the completion of the P-25 suite of standards continues to be delayed, at the same time advancements in wireless technology continue, NIJ's CommTech TWG has recommended that NIJ follow a dual path approach: both supporting development of standards in technology beyond P-25 (such as WiFi/802.11x, WiMax/806.16x and VoIP) and continuing to support P-25. We concur with them that the completion of P-25 standards, by itself, will not solve the standards problem.

NIJ's Efforts

Within existing budget constraints, and the myriad of competing technology needs of the criminal justice community, NIJ has been devoting on average $13 million per year to its CommTech portfolio. We are pleased to report that a remarkable amount of work has been done through focusing our investment. In addition to technology assistance, standards development and testing, NIJ has funded approximately 20 research, development and demonstration projects per year.

Among our accomplishments, NIJ funded the development of the Virginia Statewide Communications Interoperability Plan (SCIP), a national model for state-level planning and cooperation. NIJ worked closely with SAFECOM to develop the Virginia SCIP and continues to encourage the use of the SCIP methodology elsewhere in the nation.

One of our most notable accomplishments in the public safety communications technology arena has been funding the development of the Computer Assisted Pre-Coordination Resource and Database System (CAPRAD). This tool aids more than 50 regional planning committees to plan and use regional frequency spectrum efficiently and to better manage potential interference near jurisdictional borders. NIJ also convened a National Task Force on Interoperability and published a guidebook and pamphlet: *Why Can't We Talk* that discussed the need for federal, state and local leadership on interoperability. This publication was developed to facilitate education and discussion among and between elected and appointed officials, their representative associations, and public safety representatives on public safety wireless communications interoperability.

NIJ publishes a wide range of communications-related information for public safety professionals, such as the *Understanding Wireless Guide*, which provides a comprehensive discussion and explanation of communication systems for public safety. NIJ sponsored the development of a satellite link for the Alaska LMR system. This technology will be tested in other rural environments in the coming year under NIJ funding. The benefit of this technology in situations where the local communications infrastructure has been significantly degraded by a manmade or natural disaster is clear. However, its potential to address the more common needs of policing in rural environments with minimal communications infrastructure needs to be explored.

Through CommTech, NIJ was responsible for development of the Metropolitan Interoperability Regional System (MIRS). MIRS is designed to meet the voice communication interoperability needs of the public safety agencies in the Metropolitan Washington, DC region. It is being used extensively by federal, state, and local law enforcement agencies to aid in communication for multiple agencies in high-profile events such as the Presidential Inauguration. The MIRS testbed has produced important national benefits to public safety by improving the understanding of the benefits of communications switching technology and the pitfalls involving effective implementation of such systems.

CommTech pilot programs are unique in leveraging the participation of the vendor community by pairing a vendor with a public safety agency. NIJ partners with local law enforcement agencies and brings a specific technology to evaluate. This maximizes outcomes while simultaneously minimizing costs to the federal government. For example, NIJ is conducting a pilot program in VOIP in Danville, VA. NIJ is also exploring opportunities to initiate new pilots with SDR and wireless broadband technologies.

A major part of the CommTech program is technology test and evaluation to provide unbiased information to the public safety community. NIJ serves as an independent evaluator, trusted partner, and honest broker. These evaluations also serve to point out technology gaps that need to be filled through further research and development. NIJ has administered standards-based testing programs for criminal justice practitioners for nearly 30 years, such as its body armor testing program. Because of NIJ's body armor standard, officers have confidence in the protection afforded by their personal protective equipment. Over 3,000 officers' lives have been saved by NIJ-compliant body armor.

Public safety officials are making communications purchase decisions every day and assistance to evaluate the rapidly changing communications landscape. NIJ provides this in many ways including through our web site and publications such as the *Why Can't We Talk* guidebook and pamphlet, and our Technology In-Shorts documents.

NIJ also actively responds to technology assistance requests that we receive from public safety officials across the country. In just the last two weeks, we have responded to a request to assist with development of a communications system in Katrina-affected Mississippi and Louisiana; a technology assistance request in Haverhill, MA; and

participated in a meeting with San Joaquin, CA officials concerning communications needs. Last week, a captain of the Alexandria Police Department and a member of the CommTech team, along with staff from the National Law Enforcement and Corrections Technology Center- Southeast started to work with the Fredericksburg, VA Police and Fire Chiefs to establish interoperable communications via an interconnect switch and are addressing ways in which to optimize coverage without significant financial investment. Through the Sheriff's Association of Texas (SAT), NIJ has active and ongoing technology assistance requests with 26 Brazoria County fire departments; Frio County, Webb County, Medina County, Caldwell County, and El Paso County Sheriff's offices; and the Middle Rio Grande Development Council of Governments. NIJ is also working with SAT to further develop communications operability and interoperability for state and local agencies along the entire 26 county US-Mexico border.

CommTech provides technical support to tactical operations. CommTech provided interoperability assistance in both the 2001 and 2005 Presidential Inaugurations, Hurricane Rita response, the dedication of the World War II Memorial, and the Moussaoui trial. In May 2006, the CommTech Program will provide interoperability support for the opening ceremonies for the Woodrow Wilson Bridge via the development of an interoperability plan.

NIJ provides a critical resource to other components of DOJ related to interoperability. NIJ works very closely with the COPS Office to support their grants review process. NIJ helped to fund the DOJ Interoperability Summit in Seattle in May, 2005 and will do so again in Austin next month (May 2006). NIJ has arranged for active sworn state and local law enforcement personnel, as well as interoperability technical experts, to support all of our federal partners in interoperability efforts.

Assistance to State and Local Practitioners

NIJ's National Law Enforcement and Corrections Technology Center (NLECTC) system offers public safety agencies, both large and small, no-cost assistance in the implementation of current and emerging technologies. With a network of ten regional centers and specialty offices located across the country, the NLECTC system delivers expertise in a number of technologies including communication interoperability and information sharing. The NLECTC system plays a vital role in NIJ's CommTech efforts.

The staff of the NLECTC system's Western Center (NLECTC-West) has supported CommTech by providing subject matter experts in the field of SDR. Also, Pima County Arizona asked NLECTC-West for technology assistance in developing a communication network. The various agencies in the county use different radio systems making mutual aide interoperability difficult or impossible. Additionally, radio coverage is poor due to the mountainous terrain. NLECTC-West drafted a technical requirements document for that communication system.

The NLECTC system's Rocky Mountain Center houses the previously discussed CAPRAD database, which allows all 55 regional planning committees (RPC) to have

access to tools to coordinate their frequency planning. The RPCs also provide feedback on the CAPRAD system for continuing improvement.

Conclusion

The goal of improving public safety communications interoperability can only be achieved by dealing with the overall problem of operability. Focusing on interoperability as the only issue in first responder communications will not yield a result that will allow the responder to communicate or access information effectively.

NIJ has, at the recommendation of its practitioner-driven TWG, focused on many aspects of first responder communication operability, including interoperability. With the support of the FCC, NIJ has funded Regional Planning Councils to address local spectrum issues. It has supported the development of CAPRAD to monitor and track first responder spectrum requirements and usage across the U.S. We have supported fundamental R&D in SDR and cognitive radios in order to address issues of operability as much as interoperability. We have worked closely with the vendor community to test and evaluate the products in a real world environment and NIJ provides ongoing technology assistance through our NLECTC system.

Today, there are fundamental challenges to operability. SDR and cognitive radio technologies offer the promise to enhance communications capabilities within the current available spectrum allocations. Although new spectrum from the digital television transition will help, new technologies can help public safety to improve operability and interoperability for years to come. A single entity, or even the entire federal government, will not solve the interoperability challenge alone. There is overlap between the activities of the various federal partners for interoperability. Each represents a constituency with common as well as unique needs. Clearer delineation and better coordination among federal entities with respect to interoperability is what all of the agencies are striving to achieve. Although the challenges in public safety communications will take many years to solve, the federal government can best play a role by working towards the establishment of a comprehensive, coordinated, standards-based strategy.