



Saving Lives and Property Through Improved Interoperability

***Post-Symposium Support Report—
Atlanta, Georgia***

FINAL

December 2002

Table of Contents

1. INTRODUCTION	1
2. SYMPOSIUM TOPICS	2
2.1 Welcome and Keynote Remarks	3
2.2 The PSWN Program Update and Public Safety Wireless Interoperability National Strategy (Public Safety WINS) Video Presentation.....	4
2.3 The PSWN Program and Federal Emergency Management Agency (FEMA)—Working Together Through Project SAFECOM.....	4
2.4 Benefits of PSWN Program Assistance in Improving Interoperability.....	5
2.5 Project SAFECOM and Its Impact on Public Safety Communications	7
2.6 Evacuation During Hurricane Floyd and the South Carolina “Palmetto 800” Megahertz (MHz) System.....	9
2.7 The Status of Communications Interoperability in Georgia.....	9
2.8 Critical Communications Interoperability Requirements Between Public Safety and Other Public Services Agencies.....	10
2.9 Communications Interoperability Through Hurricane Andrew.....	12
2.10 Protecting Wireless Communications Infrastructure From Vulnerability.....	12
2.11 An Interoperability Model—Michigan’s Public Safety Communications System (MPSCS).....	13
2.12 Trooper Shot, I-20!.....	14
2.13 National Law Enforcement Telecommunications System (NLETS).....	15
2.14 Setting Up a State Interoperability Executive Committee (SIEC) for Coordinated Approaches to Improving Communications	16
2.15 The Consensus Plan Submitted by the Joint Commenters—A Plan for Spectrum.....	18
2.16 Georgia Crime Information Center	19
2.17 Commercial Media Access to Secure Public Safety Wireless Systems	20
2.18 Grants and Funding: Where to Apply for Assistance and Who Has the Money	21
2.19 Bringing Desktop Functionality to the Field with 700 MHz Wideband Data	22
2.20 Next Symposium State Presentation and Invitation	23

1. INTRODUCTION

The Public Safety Wireless Network (PSWN) Program sponsored the Atlanta Symposium October 29–31, 2002. The symposium was hosted by the Atlanta Police Department (APD). Previously, the PSWN Program sponsored similar symposiums in Charlotte, North Carolina; Harrisburg, Pennsylvania; Sacramento, California; Boston, Massachusetts; Chicago, Illinois; Mesa, Arizona; Denver, Colorado; Lansing, Michigan; Orlando, Florida; St. Louis, Missouri; Honolulu, Hawaii; Boise, Idaho; Minneapolis, Minnesota; Las Vegas, Nevada; Charleston, South Carolina; and Portland, Oregon. The three-day conference was composed of panels and group discussions addressing many of the technical, political, and financial issues challenging interoperability today.

This report provides a detailed summary of the events of the Atlanta, Georgia, PSWN Program Symposium. It is designed to be a historical resource for those who attended the symposium and to provide a broad overview for those who were unable to attend. In general, this symposium report highlights—

- Key presentations and panels discussed during the symposium
- Interoperability challenges and success stories that were discussed throughout the symposium
- Important facts and information that were provided to the audience.

The remainder of this report consists of 20 sections addressing the topics of each panel discussion and presentation at the symposium.

2. SYMPOSIUM TOPICS

The information on each topic area presented in this section was provided through presentations and panel discussions from members of the public safety community and the PSWN Program representatives. The topics were selected to give the symposium attendees a perspective on the PSWN Program and efforts to improve communications interoperability. The topics covered are listed below:

- Welcome and Keynote Addresses
- The PSWN Program Update and Public Safety Wireless Interoperability National Strategy (Public Safety WINS) Video Presentation
- The PSWN Program and Federal Emergency Management Agency (FEMA)—Working Together Through Project SAFECOM
- Benefits of PSWN Program Assistance in Improving Interoperability
- Project SAFECOM and Its Impact on Public Safety Communications
- Evacuation During Hurricane Floyd and the South Carolina “Palmetto 800” Megahertz (MHz) System
- The Status of Communications Interoperability in Georgia
- Critical Communications Interoperability Requirements Between Public Safety and Other Public Services Agencies
- Communications Interoperability Through Hurricane Andrew
- Protecting Wireless Communications Infrastructure From Vulnerability
- An Interoperability Model—Michigan’s Public Safety Communications System (MPSCS)
- Trooper Shot, I-20!
- National Law Enforcement Telecommunications System (NLETS)
- Setting Up a State Interoperability Executive Committee (SIEC) for Coordinated Approaches to Improving Communications
- The Consensus Plan by the Joint Commenters—A Plan for Spectrum
- Georgia Crime Information Center

- Commercial Media Access to Secure Public Safety Wireless Systems
- Grants and Funding: Where to Apply for Assistance and Who Has the Money
- Bringing Desktop Functionality to the Field with 700 MHz Wideband Data
- Next Symposium State Presentation and Invitation—Los Angeles County Fire Department and Sheriff’s Department, California (January 2002).

The following sections present each topic, supported by the remarks of the presenters.

2.1 Welcome and Keynote Remarks

At the Atlanta Symposium, 169 public safety officials from around the country assembled to discuss various topics relating to public safety wireless communications interoperability. Public Relations Officer Jolene Butts Freeman of the Atlanta Fire Department (AFD) and Deputy Chief William B. Shannon, Atlanta Police Department (APD), provided welcoming remarks. District Three City Councilman Ivory Lee Young made the keynote address.

Ms. Freeman welcomed the PSWN Program and the symposium attendees to Atlanta. She gave a brief history of the City of Atlanta and described how the public safety community served the citizens of Atlanta. She also commented that the city continued to strive for greater interoperability. She closed by again welcoming everyone to the City of Atlanta.

Deputy Chief Shannon also extended a warm welcome on behalf of the APD. He began by stating that the word going around was interoperability. He said that for a long time it had been a goal of the police and fire agencies to achieve interoperability and that the City of Atlanta had one of the premier interoperability systems in the country. He stated that it was imperative that interoperability be maximized in order to minimize the possibility of miscues in day-to-day communications. Deputy Chief Shannon also introduced Councilman Young.

Councilman Young thanked the public safety agencies represented by the PSWN Program, symposium attendees, and the citizens of Atlanta. He pointed out that on a daily basis, public safety personnel put their lives at risk to protect the citizens they served. He continued by stressing the importance of the symposium for the public safety personnel here today. Councilman Young continued by stating that most were neophytes regarding the issues of homeland security and insisted that everyone must approach the solution to this challenge with a sense of humility and humanity. Mr. Young closed by identifying technology as the basis for providing a safer community and stating that everyone must come together to battle terrorism and local injustices.

2.2 The PSWN Program Update and Public Safety Wireless Interoperability National Strategy (Public Safety WINS) Video Presentation

Mr. Bob Lee, PSWN Program Manager for the Department of Justice (DOJ), provided an overview of the critical challenges to improving interoperability. He began by stating that wireless communications interoperability was necessary to improve the ability of the public safety officers to save lives and property, facilitate rapid and efficient interaction among all public safety organizations, and provide immediate and coordinated assistance in day-to-day missions, task force operations, and mass casualty incidents. He added that the events of September 11 had highlighted the necessity for effective public safety operations and that the ability to communicate heavily impacted the effectiveness of public safety first responders.

Ultimately, Mr. Lee said, effective communications was a key component of homeland security. The ability to communicate was important in saving lives and protecting property because it made possible incident command and control, dissemination of information in real time to areas in need, improvement in evacuation coordination, and reduction in casualties.

Mr. Lee then described the PSWN Program and what it was doing to improve public safety wireless communications interoperability. For further information on the program, visit the program's Web site at www.pswn.gov.

2.3 The PSWN Program and Federal Emergency Management Agency (FEMA)—Working Together Through Project SAFECOM

Ms. Susan A. Moore, Project Manager, Project SAFECOM, began by pointing out that public safety had become vulnerable because of jurisdictional boundaries on information and shorter deadlines available to access that information. She proceeded with a presentation on Project SAFECOM. Ms. Moore described the program as—

- A priority E-Government initiative established by the Office of Management and Budget; approved by the President's Management Council
- A government-to-government initiative with the objective of making it easier for states and localities to participate as full partners with the Federal Government to provide citizen services.

Ms. Moore stated the project mission was to enable public safety personnel nationwide to improve citizen response through more effective and efficient communications. She continued by listing the three top priorities of Project SAFECOM:

- Provide central coordination and reference materials for existing interoperability solutions
- Facilitate state and local access to resources and funding to implement interoperability solutions
- Identify practitioner requirements and develop strategic direction for next generation solutions.

Ms. Moore identified the challenges that faced the public safety community and said that the PSWN Program would play a central role in Project SAFECOM. Supporting that statement, she said, “The PSWN Program has a healthy baseline of information and resources to assist the public safety community and we, Project SAFECOM, plan to follow through with this same effort.”

Ms. Moore explained that the effort would include organizing and implementing interoperability solution work packages. The work packages consisted of the following elements:

- Requirements
- Gap Analysis
- Concept of Operations
- Technology Solutions
- Strategic Plan
- Funding/Grants/Contracts
- Outreach
- Policy.

Ms. Moore closed by listing three ways that public safety agencies could help with interoperability success: contribute experience and needs, serve as advocates for the program, and move into action—implementation.

2.4 Benefits of PSWN Program Assistance in Improving Interoperability

This panel discussed the benefits the panelists experienced by working with the PSWN Program to improve interoperability in their locales, states, and regions. Major William Gordon (APD) moderated the panel. The following are highlights of the panel discussion:

- Lieutenant Colonel David Felix, Assistant Director, Arizona Department of Public Safety, began the discussion by describing the first symposium he attended in Boise, Idaho. He stated the PSWN Program assisted the State of Arizona in—
 - Moving forward with a statewide system and interoperability effort
 - Understanding the role of the state and how that role fit into interoperability
 - Understanding how the state could participate in 700 MHz spectrum coordination
 - Acquiring funding and where the resources were
 - Implementing outreach and educational programs.

He also described how the PSWN Program assisted the state with sponsoring symposiums in the northern and southern parts of Arizona. Lieutenant Colonel Felix closed by stating that the Governor of Arizona was moving forward with statewide public safety communication systems and that education had been a key ingredient.

- Mr. Michael Bennett, Director, Electronic Services Section, Maryland State Police, explained how the State of Maryland had planned for years to implement a statewide

800 MHz communications system, but the funding never worked out. He pointed out that the State of Maryland had hosted the first one-day symposium and that the Maryland Incident Management Interoperable Communications System had blossomed from that partnership. He stated that the PSWN Program assisted the State of Maryland in—

- Raising awareness
- Implementing outreach and educational programs
- Establishing partnerships.

He explained that Maryland had a very high frequency (VHF) lowband system and that bordering cities were preparing to install 800 MHz systems. He stated that the need to interoperate with them was essential, and he considered the PSWN Program an invaluable resource in learning how to accomplish interoperability. Mr. Bennett closed by offering the symposium attendees the solutions and lessons learned in the State of Maryland.

- Mr. Gary Cochran, Assistant Bureau Chief and Starcom21 Project Manager, Illinois State Police, stated that the Illinois State Police were pursuing an initiative called Starcom21. He explained how the state had funded an 18-month study to develop a \$240 million ultra high frequency (UHF) statewide system and realized there was insufficient funding to support this effort. As a result, Mr. Cochran explained, the state had taken another look at their communication needs and decided to look to the PSWN Program for assistance. He stated that the PSWN Program assisted the State of Illinois in—
 - Developing requests for proposals
 - Raising funding through various resources
 - Developing effective proposals for the state appropriation committees.

Mr. Cochran stated that what came out of the partnership with the PSWN Program was \$25 million in funding, a state committee of 250 people, and a three-level vendor selection process. He closed by stating that Motorola designed a system that provided 95 percent mobile coverage, 95 percent portable in-building coverage (in specific locations and buildings), 186 tower sites to achieve portable coverage requirements, and a delivery date of September 28, 2004.

- Mr. Robert Hlivak, Radio Engineer, Information and Communication Services Division State of Hawaii, began by explaining that he worked for the infrastructure division of communication services, which focused on how the communications system was connected. He explained that the State of Hawaii presently used Motorola and EF Johnson systems, which employed various frequency bands in the spectrum. Mr. Hlivak pointed out that the neutral environment was the most important aspect of the symposiums sponsored by the PSWN Program. He clarified that the symposiums were not federal, state, or local; instead, they focused on people working together. He said that the PSWN Program assisted the State of Hawaii by—

- Providing a cost/benefit analysis for a statewide system
- Making it possible to have a direct access to the state government representatives.

Mr. Hlivak reported that an interoperability assistance solution sponsored by the PSWN Program was in operation and people were talking with each other. He stated that the solution consisted of a few ACU-1000s placed throughout an operational region. He pointed out that as the partnerships were developed and the system was designed, the state, local, and federal systems needed to be meshed together. He qualified this by explaining that even if one of the agencies were to pull out of the partnership, the system would remain fully functional because it did not completely rely on any one agency. Mr. Hlivak closed his discussion by stating that attendees needed to talk to each other during the symposiums, even if nothing else was done so they could learn from each other.

2.5 Project SAFECOM and Its Impact on Public Safety Communications

Mr. Michael Duffy, Director, Telecommunications Services Staff, DOJ, began his presentation by stating that the Integrated Wireless Network (IWN) program was a strategic effort to implement standards-based technology and that its planners hoped to encourage other public safety agencies to invest in standards-based technology as well. He also stressed that the effort was in line with the National Telecommunications and Information Administration (NTIA) mandate for federal agencies to migrate to the narrowband standard. He then defined IWN in the following terms—

- Collaborative effort between the Department of the Treasury and the Department of Justice
- Multi-agency, standards-compliant wireless communications service
- Outgrowth of separate efforts initiated in the two departments to replace aged equipment, improve interoperability, and meet the NTIA narrowband mandate
- Network of approximately 2,500 radio sites around the country.

Mr. Duffy identified the key architectural elements of IWN as—

- Association of Public Safety Communications Officials (APCO) Project 25 compliant
- Primarily VHF (UHF used in prisons and selected seaports and airports)
- Trunked radio
- Internet Protocol (IP) based integrated voice and data infrastructure
- Over-the-air rekeying
- Commercial services to augment Government-owned land mobile radio.

Mr. Duffy also identified the key system attributes as—

- Trunked radio capabilities throughout the system
- Ninety-five percent coverage in prescribed service areas
- Grade of Service (ability to get service within 1 second)—99 percent in metropolitan, border, and “campus” areas and 90 percent in rural, highway, and Native American land areas
- Continuous portable coverage provided within five miles of borders (mobile coverage would extend further—approximately 20–30 miles)
- Portable coverage provided in metropolitan areas and campus settings (e.g., prisons and airports)
- Ability to “roam” across areas and zones
- Interoperability gateways for connectivity to state and local systems, as well as for transition from legacy systems.

Mr. Duffy explained some of the underlying reasons why the Departments of the Treasury and Justice were consolidating their systems. He explained that both agencies had equipment that required replacement due to age and frequency of failure, and that they had similar missions and operational areas. He concluded that IWN would initially be deployed as a pilot by January 2003 to see how well a large number of local, state, and federal agencies could actually talk to each other. He said that the general strategy would be to move across the northern border. He then opened the floor for questions.

The following questions, answers, and comments were presented:

1. What is your time frame to implement the buildout of the IWN system if the pilot is successful?
Mr. Duffy replied that the buildout would begin a year from now, and the overall time frame for the complete system buildout was eight years. He added that the program should be funded by then to begin the implementation.
2. Are you concerned that after all this effort that we may end up back where we are today?
Mr. Duffy replied that this was a large project and would require some creativity to make it happen. He said they expected challenges throughout its implementation, but emphasized that the project had to move forward.
3. What are the in-building coverage requirements for metropolitan areas?
Mr. Duffy replied that this would be determined on a city-by-city basis.

4. Could you elaborate on the status of the narrowband mandate and do you expect state agencies to follow?

Mr. Duffy replied that the narrowband mandate for VHF must be met by January 1, 2005, but that attendees should get specific information from NTIA. He added that there were a number of federal agencies that would not meet the mandate due to funding issues. He also suggested that if the state and local agencies met the narrowband mandate, it would increase the probability of success for national interoperability.

Mr. Don Speights, Public Safety Program Manager, NTIA, added that funding was an impediment to the federal agencies in meeting the mandate, but there was no mandate currently for state and local agencies. He agreed with Mr. Duffy's suggestion for state and local agencies to increase their chances for achieving interoperability.

Finally, Mr. Duffy stated that the general requirements were being developed as pilots and tested based on the technical solutions and partnerships that presently existed.

2.6 Evacuation During Hurricane Floyd and the South Carolina "Palmetto 800" Megahertz (MHz) System

Lieutenant J.D. Connelly, Research & Development Unit / Patrol Supply, South Carolina State Patrol, began by providing a brief history of the patrol officers' communication methods. He identified Hurricane Hugo, Hurricane Floyd, and the Charleston Riots as the three pivotal incidents that led to the realization that a statewide system and interoperability were needed for public safety agencies in the State of South Carolina. He explained that the state transition from a VHF lowband system to an 800 MHz system and the creation of advisory committees were two steps the state took as a result of the hurricanes and riots. Lieutenant Connelly opened the floor for questions or comments.

The following were questions and answers during this presentation:

1. If the system were to fail, what mechanisms are in place that respond to environmental survivability?

Lieutenant Connelly replied that if one of the state-owned sites was damaged, the state would be responsible for the repairs. He explained that the state was installing generators and other backup equipment at the sites where public safety equipment was installed and that there was language in the contract agreement that addressed these issues.

2. Who manages the users and the programming on the system?

Lieutenant Connelly stated that his committee took care of talk group and feature assignments and programming prior to an agency joining the system.

2.7 The Status of Communications Interoperability in Georgia

Mr. Wray Hall, State Frequency Coordinator, Georgia Technology Authority, presented information about the status of communications interoperability in Georgia. He listed the

highlights of his presentation as current system usage, shared spectrum, future plans, issues, and open discussion. He listed the State of Georgia channels as—

- Intrastate Coordination Channels
- Mobile Radio District Channels
- Nationwide 155.475 MHz
- Statewide VHF/UHF channels
- Regional assignments
- Many hospitals and emergency medical services (EMS) on county or local systems
- Narrowband 12.5 kilohertz (kHz)
- VHF pairs—CALL/TAC-1 to TAC-4
- UHF pairs—CALL/TAC-1 to TAC-3
- National Public Safety Planning Advisory Committee (NPSPAC) 821 MHz Region 10—Georgia
- Mutual Aid (821 MHz).

Mr. Hall explained that cross-jurisdictional communications were implemented by creating local agreements, identifying and using shared channels, and trading radio equipment. He then explained that the future plans for Georgia consisted of acquiring a statewide radio system, developing seamless interoperability at all levels, forming a state interoperability committee, and developing a statewide plan for the 700 MHz frequency spectrum. He concluded by pointing out that the issues facing the state were participation, funding, approvals, implementation, and cooperation.

2.8 Critical Communications Interoperability Requirements Between Public Safety and Other Public Services Agencies

Mr. Richard Butler, Senior Police Officer and COMNET Coordinator, Atlanta State Police, explained that COMNET was a communication network in partnership with corporate Atlanta. He added that it was an extension of public safety's resources created by partnering with private security officers located throughout the city. He said that the COMNET user agreement allowed federal, state, local, and private users to communicate directly with the state police.

Senior Officer Butler provided a video presentation on COMNET. The video stated that 10 years ago, COMNET was a solid concept that worked well in other locations. As a

consequence, the City of Atlanta implemented COMNET, and it had assisted in the apprehension of more than 4,000 criminals. The video listed the following COMNET characteristics:

- Members must be willing to prosecute on all calls, and appear in court as required
- Business must be in city limits of Atlanta
- Members must provide necessary radio equipment
- Members meet quarterly to discuss important issues, review current and past performance, and share information
- A Steering Committee composed of representatives of COMNET members served as the governing body and administrative resource for the network
- Member companies paid a membership fee of \$100 per year, earmarked for the maintenance of the network and a \$50 charge for each additional location or site.

Mr. John Player, Lieutenant, Metropolitan Atlanta Rapid Transit Authority Police, explained that his department purchased a mobile command post and installed an ACU-1000 to provide interoperability between multiple agencies. He stated that operating procedures were being developed. He further explained that when criminals were observed crossing jurisdictions, the observing officer could contact the local dispatch center through the ACU-1000 and receive an immediate response. He closed by emphasizing that during the design of a statewide system, planners should spend some time with the 911 dispatch centers because the dispatchers were the first responders in any situation.

Mr. Jim Cook, Director, Fulton County Emergency Management Agency, began by stating that interoperability was a major issue with his agency. He said that it was his agency's responsibility to organize the mobile command post so that different organizations could have interoperability with each other. He closed by stating that personnel communicated with other jurisdictions on a daily basis.

The following questions, answers, and comments were presented:

1. Have you run into a situation where you needed priority access?
Mr. Cook explained that the software used had a special option to deal with situations in which a busy signal was received. He said the software would dial around the problem until it found an unengaged telephone number and then accessed the system.
2. What happens if a radio is lost or stolen?
Mr. Cook stated that the 800 MHz system had a unique ID (hexadecimal code) so that a lost or stolen radio could be identified; however, the UHF system did not have that capability.

3. How do you communicate with the public users if they do not understand the standard 10-codes?

Mr. Cook explained that agencies in Georgia were transitioning into a plain text language so that everyone could understand each other.

2.9 Communications Interoperability Through Hurricane Andrew

Mr. Alfred (Rocky) Moore, Director, Fulton County Emergency Services Department, began by providing an overview of the damage caused by Hurricane Andrew, which hit Miami, Florida, on August 24, 1992. He stated that after the storm hit, the public safety community was faced with the effort to coordinate resources, perform search and rescue, and conduct radio communications while facing the same total devastation as the citizens themselves. He identified the lessons learned from this disaster—

Lessons Learned

- In order to evacuate the population quickly, use the northbound and southbound lanes to move traffic out of Florida
- There are no safe places during a storm of that magnitude
- A recovery plan needs to be in place

Mr. Moore stated that there were a number of efforts by private radio manufacturers, cellular companies, and the Governor of Florida to assist in the recovery, but there was no communications coordination. He said that initially, the police and the fire personnel worked independently with no coordination. Mr. Moore explained that even after a temporary communications solution was in place and recovery was occurring, the morale of the public safety personnel quickly diminished due to fatigue. He emphasized to the symposium attendees that a recovery plan must be in place, and the communications system should be tested under crisis conditions. Mr. Moore closed by re-emphasizing that multiple public safety agencies needed to coordinate and work together. He opened the floor for questions and comments.

The following question and answer was presented:

1. When will the police and fire start talking to each other in your region?
Mr. Moore replied, “You would think after this devastating storm and new system installation, they would be talking to each other.” He added that the fire department felt that the EDACS system did not provide the coverage they needed so they chose not to use it.

2.10 Protecting Wireless Communications Infrastructure From Vulnerability

Mr. David Perry, Global Director of Education, TrendMicro, explained the vulnerabilities facing public safety communication networks and what attendees could do to protect their systems. He began by defining three forms of computer viruses that could cause a computer system to fail. He defined a virus as anything that replicated itself without authority, a worm as a virus that moved itself from computer to computer, and a Trojan horse as a virus that typically came in through e-mails and was an executable. He predicted that wireless viruses would take over the virus battleground in the future.

Mr. Perry closed by advising attendees to access only trusted virus Web sites (i.e., Symantec and McAfee) and avoid Web pages claiming to provide the latest on viruses, indicating that these sites frequently contributed to spreading viruses rather than stopping them. In addition, he offered the following Web site as another good source of information on viruses: www.wildlist.org.

2.11 An Interoperability Model—Michigan’s Public Safety Communications System (MPSCS)

Captain Tom Miller, Captain, Michigan State Police, began by stating that the PSWN Program had been instrumental in many of the state’s efforts. He discussed the challenges and successes in planning and developing the MPSCS. He said the State of Michigan had been a leader in the development of statewide systems for years, and the Michigan State Police served as the lead agency in developing a digital, trunked, Project 25-compliant, 800 MHz system for use by all state agencies and interested federal agencies and local governments. The primary vendor for the system was Motorola. The key feature of the system was that it provided intra-agency interoperability statewide. Captain Miller stated that Michigan was funded to provide the infrastructure, while federal and local agencies that wanted to participate on the system provided the end-user equipment. He reported that the system was costing the state approximately \$221 million.

Captain Miller said Michigan’s system was being developed in four phases. The first three phases were complete, and 120 tower sites were operational. He indicated that phase four covered the upper east and west peninsula of Michigan and that 61 towers were under construction. He reported that the system currently had more than 64,000 user identifications and 16,000 talk groups on all levels of government. Captain Miller stated that new participants discovered the benefits of a shared system and incurred only minimal cost to use the backbone of the statewide system. He said that the final phase would be completed by the end of 2002. Captain Miller provided the following lessons learned from Michigan’s experience:

Lessons Learned

- A solid contract is critical
- User expectations must be managed
- Little problems become the biggest
- Field beta test, if possible
- People make the project
- Communication inside and outside the Project Team is essential
- Focus on training
- Property is the white elephant

The following questions, answers, and comments were presented:

1. What test platform are you using to certify the different vendors' equipment?
Captain Miller stated that he would provide the questioner with the test plan.
2. Do you have a built-in mechanism for equipment replacement?
Captain Miller replied that the fees charged went directly to a state fund, and the division that maintained the system did not manage those funds.
3. Do you generate revenue from system leasing?
Captain Miller stated that the state did not generate any revenue from the system. He added that the communications division intended to manage system capacity for public safety users and not for private companies.
4. Do you maintain the programming of the system components?
Captain Miller stated that communications division personnel performed all programming and maintained the templates for the radios and fixed equipment. He added that they also maintained the system keys.
5. Do the rural agencies use your system as their primary system or are they using a secondary system?
Captain Miller stated that most of the smaller agencies were still rural and still used their own system, but the state was in the process of adding new sites to provide coverage in the rural areas.

For more information on the Michigan system, visit its Web site at www.mpscsc.com.

2.12 Trooper Shot, I-20!

Ms. Tracy Roberts, Radio System Manager, 800 MHz Department, Cobb County, Georgia, identified the current status, needs, studies, and goals for obtaining interoperability as key elements facing Cobb County with its interoperability goals. She stated that the public safety agencies in Cobb County operated using different frequency bands and system architectures.

Ms. Roberts said that, "Interoperability among public safety responders can be measured in lives." She emphasized that the county would obtain interoperability by promoting effective public safety communications, fostering interoperability, acquiring common technology standards, defining seamless interoperability, and developing cost-efficient approaches.

The following questions and answers were presented:

1. What type of system do you presently use?
Ms. Roberts replied that Cobb County used a three-site Motorola SmartNet simulcast system and that the system needed to be expanded.
2. Do you see a dual band system being implemented in your area?

Ms. Roberts stated that they were migrating in that direction.

3. Are all the 800 MHz systems in your area built by the same manufacturer?

Ms. Roberts stated that the systems were built by the same manufacturer, and the county was presently drafting an agreement to which local agencies would agree in order to ensure a single manufacturer for future system purchases.

2.13 National Law Enforcement Telecommunications System (NLETS)

Mr. Gib Heuett, Assistant Deputy Director, Georgia Crime Information Center, Georgia Bureau of Investigation [GBI], presented information on NLETS, which ties local, state, federal, and international criminal justice agencies together to share information. He stated that the system provided access to customs data, Internet fraud data, missing children posters, images, fingerprints, and other criminal justice related information. He pointed out that NLETS did not store and maintain the information but provided a nationwide network to access databases stored at different agencies' locations. Mr. Heuett described NLETS in the following terms:

- NLETS is a not-for-profit corporation
- It is located at the Arizona Department of Public Safety
- The members are all states and federal agencies
- NLETS is managed by its criminal justice users
- It carries Federal Bureau of Investigation (FBI)-III traffic throughout the United States and Canada
- NLETS operates 24 hours a day, seven days a week, 365 days a year
- Message delivery is guaranteed
- Priority message queuing is used
- NLETS has a national "ALERT" messaging system for all points bulletins
- NLETS is creating the Standardized National Rapsheet in XML to establish a single nationwide standard
- NLETS partners with Royal Canadian Mounted Police and the FBI for international connectivity.

Mr. Heuett explained that technology was not the issue, but that coordination and administration of the information and working together to standardize the information was key to the success of the system. He stated that Georgia, because of its partnership with NLETS, was a hub of information and provided more than 10,000 end users with information. He closed by

encouraging more public safety agencies to get on the system so that more information would be available throughout the country.

The following questions and answers were presented:

1. Do you see a problem with sharing information with non-members (e.g., railroad facilities)?
Mr. Heuett explained that Georgia provided agencies the information, but not hard copies. He added that sharing the information with agencies was critical and great care was exercised. He agreed that it was possible for unauthorized persons to obtain information but that exchange could not stop because of this possibility.
2. Does NLETS have any guidelines?
Mr. Heuett replied that public safety agencies needed to define these guidelines and the information that was available.
3. Can you explain the connection between the hazardous material agencies and NLETS?
Mr. Heuett explained that for this particular application, NLETS was used as a tool to provide information about hazardous material to personnel that were not familiar with these materials.
4. What level of encryption do you use?
Mr. Heuett replied that 128-bit encryption was used because of agency limitations.
5. Is there still a prohibition on criminal history information being sent over networks?
Mr. Heuett stated the he believed the prohibition had been lifted and this issue was handled on a system basis and a log was kept of the transactions.

2.14 Setting Up a State Interoperability Executive Committee (SIEC) for Coordinated Approaches to Improving Communications

Mr. Clark Palmer, Division Manager, Washington State Patrol, began his presentation by stating that public safety agencies at all levels of government required communications interoperability in both routine and emergency operating environments. He said the Washington State SIEC was established to—

- Monitor public safety agencies' need to upgrade, expand, and enhance voice and data wireless capacity
- Provide the access public safety and justice agencies need to communicate with other state, local, or federal wireless systems
- Provide policy guidance and direction regarding wireless voice and data system development.

In addition, Mr. Palmer said the SIEC was intended to serve as a centralized forum to address wireless interoperability issues and encourage development and modification of systems (e.g., voice and data) within a state. The central objectives of SIECs were to promote systems development that maximized economies of scale and to initiate consolidated procurement and maintenance activities. He pointed out that the Federal Communications Commission (FCC) had also made formation of an SIEC, or its equivalent, a prerequisite for states obtaining licenses for the 2.4 MHz of spectrum designated for state licensing on the 700 MHz band.

Mr. Palmer listed a number of lessons learned from Washington State's experience in forming an SIEC:

Lessons Learned

- Discussions take place in the different "languages": policy level, technical detail, and executive level (find and use experts in each area)
- SIEC creation and maintenance is resource intensive
- Issues will arise: SIEC membership turnover, changing priorities, funding constraints, turf wars, etc.
- It has taken decades to create the problem; it will not be fixed in a week
- Looking for common ground, as the basis for all discussions, is key
- A communication plan is critical to preserve the momentum
- Continuous education and outreach is required for success
- Policy-level representation is needed on the committee.

Mr. Palmer stressed the need to establish subcommittees to carry out the actual technical work and preserve the momentum, and said that these subcommittees must have the authority to meet regularly. He cited the current Washington State SIEC director's policy of having a deliverable for every two of these meetings to show tangible work product versus mere discussion. Mr. Palmer closed by saying that continual outreach was a key component of success, as were scalability, increasing the scope of SIEC activities, the experience base, participation, and challenges regarding SIEC activity.

The following questions and answers were presented:

1. Why did you decide to enhance your microwave system instead of going with a technology like voice-over IP (VoIP)?
Mr. Palmer explained that they were going to VoIP eventually, but needed to have the digital backbone in place to handle it.
2. Did you find a reasonable way to reach out to the tribal and federal groups?
Mr. Palmer stated that after meeting with the FBI and various tribal entities, they found that the tribal police were the best common ground.
3. Have you looked at possibly forming corporate partnerships with companies like Microsoft to discuss the possibility of funding initiatives?
Mr. Palmer stated that they typically looked for partnerships with radio manufacturers.

2.15 The Consensus Plan Submitted by the Joint Commenters—A Plan for Spectrum

Mr. Don Speights, Public Safety Program Manager, NTIA, and Kathleen O'Brien Ham, Deputy Bureau Chief, Wireless Telecommunications Bureau, FCC, provided presentations on how each organization was addressing public safety spectrum issues.

Ms. O'Brien Ham began by explaining some of the broad tasks the FCC performed, which included licensing every public safety and private organization, managing the spectrum, and handling interference issues on a case-by-case basis. She stated that handling interference issues was a growing problem so the FCC had developed a best practices guide, which was posted on the FCC Web site (see <http://www.apco911.org/frequency/downloads/BPG.pdf>).

Ms. O'Brien Ham added that Project 39 was the best practices guide to assist licensees and system designers when implementing communication systems. She explained that the interference issues were primarily due to the change in technology. She added that there was a collision course between users of Nextel's 800 MHz spectrum and public safety's 800 MHz spectrum and that the FCC was sensitive to this progression. Ms. O'Brien Ham said that solutions were being addressed by setting standards for better receiver sensitivities and stricter transmitter emissions. She stated that a group of parties, which consisted of public safety and private carriers, developed a consensus plan, "Public Safety Organizations and Private Wireless Coalition," to address spectrum issues between public safety and private carriers.

Ms. O'Brien Ham also listed some current spectrum initiatives:

- Changing the NPSPEC channels to the 821–824 MHz band
- Implementing a 2 MHz guard band for the 809–814 MHz band
- Allocating 75 MHz of spectrum in the 5.9 gigahertz band for short-range wireless communications links to transportation system equipment and roadside service vehicles to permit more efficient deployment of response to traffic incidents and emergencies
- Using spectrum below 512 MHz at the low end more effectively. Approximately 300,000 letters concerning how this band could better be used were sent out, and the FCC has received more than 33,000 letters back with call signs of unused channels. This allowed the FCC to make this spectrum available for reallocation. For more information, visit <http://www.wireless.fcc.gov/plmrs/audit.html> or for questions, contact Mary Shultz, Chief, Licensing and Technical Analysis Branch, Public Safety and Private Wireless Division, (717) 338-2656.

Mr. Don Speights explained that NTIA was the federal (Executive Branch and licensing body) component of the FCC. He stated that several proposals had been submitted by private carriers and public safety agencies to resolve interference problems and spectrum reallocation. Mr. Speights said that public safety had learned it was better to solve rather than mitigate the problem. Several comments were made by symposium attendees regarding specific spectrum concerns and were addressed by Mr. Speights. He explained that 255 MHz of federal spectrum

and 245 MHz of Department of Defense (DoD) spectrum was being provided, but that it was not contiguous spectrum, which was another problem in itself. He also stated that the Congress was reviewing the possibility of removing an additional 255 MHz from the DoD for reallocation, but this had not been settled.

This panel illustrated the difficulties involved in solving interference problems and pointed out the ultimate responsibility of the FCC to find an overall solution.

2.16 Georgia Crime Information Center

Mr. Paul Heppner, Deputy Director, Georgia Crime Information Center [GCIC], GBI, provided a detailed presentation on the services provided by the GCIC. He explained that services provided by the GCIC were handled using the Criminal Justice Information Technology Network. He explained that officers had direct access to resources in the United States and internationally through the National Crime Information Center and NLETS.

Mr. Heppner identified the following seven primary services provided by the GCIC:

- Data exchange using mobile data terminals and computer aided dispatch (CAD)
- Geographical maps in conjunction with the CAD systems to help dispatchers provide quicker service
- Automated Fingerprint Identification System to provide updates on fingerprint records within 15 minutes of booking
- Laboratory Management Information System
- Sex Offender Registry
- Protection Order Registry, a Web-based system to allow the user to see the actual order
- Firearms Program, which required that prior to purchasing a firearm, an individual must register with the GCIC for a background check.

Mr. Heppner closed by identifying information sharing as a critical and essential component in addressing criminal and natural disaster situations, but adding that criminal justice agencies must work together to standardize the information.

The following questions and answers were presented:

1. Who scans in the court order documents?

Mr. Heppner explained that the courts were responsible for scanning the documents into the database, but the Sheriff's Department was responsible for validating the record.

2. GCIC implemented 128-bit encryption. Can you speak about any examples of using it?

Mr. Heppner stated that 128-bit encryption was still in the development stage and would be part of the statewide rollout planned for 2005.

2.17 Commercial Media Access to Secure Public Safety Wireless Systems

Chief William Carrow, Communications Chief, Delaware State Police, discussed how the State of Delaware allowed the public, media, and other public safety agencies to listen to their radio communications. He said that monitoring by the public was for pleasure or profit, by the media because it feel it had an inherent right to listen to public safety operations, and by other public safety agencies to monitor mutual-aid channels. He stated that monitoring day-to-day police and fire operations was not a problem, but monitoring covert operations and federal operations was a big concern. Chief Carrow explained that Delaware used policy and procedure, talk group authorization, vendor-direct equipment purchase, and programming to address the monitoring requests by the media and public. Chief Carrow explained that state police developed a Web-based monitoring tool for the media and public to listen to traffic on the public safety system.

Chief Carrow described Delaware's current public safety communications system. He said it was a true statewide trunked digital public safety system 800 MHz system that provided communications for the following organizations:

- Police, Fire/EMS
- Department of Corrections
- Delaware Department of Transportation and transit buses
- Federal agencies
- Public utilities
- Delaware Emergency Management.

Chief Carrow said the system cost was \$52 million.

He then introduced a method of retrieving lost or stolen radios instead of having to purchase a new radio. He explained that their method forced the missing radio into a special talk group and then encouraged the individual who had the radio to return it and receive a reward with no questions asked. He closed by stating that every agency should have a policy and procedure in place to address the growing interest in public safety monitoring by the media and public. He told the attendees that the Delaware Public Safety communications system could be monitored at www.state.de.us/dsp.

The following questions and answers were presented:

1. Why is it important to have a policy and procedure in place?
Chief Carrow stated that Delaware had to put a policy in place because the media were overwhelming public safety agencies with information requests.

2. Do you provide audio from investigations after the investigations are closed?
Chief Carrow stated that the Deputy Attorney General had to authorize release of this type of information.
3. Do you follow the method of encryption key management that the PSWN Program recommends?
Chief Carrow stated that system users would like to have over-the-air-rekeying because it was extremely time consuming to go out and reprogram.
4. Do the different agencies on your system use the same encryption key?
Chief Carrow stated that all of the agencies on the system used the same encryption key, and the Delaware State Police now purchased radios that could hold two keys.
5. What type of encryption is used?
Chief Carrow stated that Digital Encryption Standard Excel from Motorola was used, and the state police would test EF Johnson radios on the system to validate encryption operation.

2.18 Grants and Funding: Where to Apply for Assistance and Who Has the Money

Corporal Bruce Clemonds, Grants Projects Special, Missouri State Police, encouraged symposium attendees to look beyond traditional sources of public safety funding (e.g., DOJ) to others such as Department of Education and the Department of Transportation for grants to assist with public safety communications as a component of supporting these agencies' missions. He added that state and local applicants could pool grants from multiple sources to address joint communications needs.

Corporal Clemonds pointed out that online resources were valuable research and application tools as the grant process moved away from traditional paper-based activity. He added that, *several grants could only be applied for online*. Corporal Clemonds provided the following list of these online resources:

Funding Resources

<http://www.fedbizops.gov> (Federal Business Opportunities)
<http://www.firstgov.gov> (Federal Government Grants)
<http://www.ojp.usdoj.gov/BJA/> (Bureau of Justice Assistance)
<http://www.ojp.usdoj.gov/nij/funding.html> (National Institute of Justice)
<http://ojjdp.ncjrs.org/grants/grants.html> (Office of Juvenile Justice and Delinquency Prevention)
<http://www.ojp.usdoj.gov/ovc/fund/welcome.html> (Office for Victims of Crime)
<http://www.ojp.usdoj.gov/bjs/funding.htm> (Bureau of Justice Statistics)
<http://www.ncjrs.org/fedgrant.html> (National Criminal Justice Reference Service)
<http://www.usdoj.gov/cops/gpa/default.htm> (U.S. DOJ Response Center)
<http://www.opm.state.ct.us/pdpd1/grants/llebg.htm> (Local Law Enforcement Block Grants)
<http://fr.cos.com/Docs/aboutfr.shtml> (Federal Register)
<http://www.cfda.gov/> (Federal Domestic Assistance Catalog)
<http://fdncenter.org/funders/> (Foundation Center)
<http://www.cof.org/resources/grantresources/index.htm> (Council on Foundation Center)
<http://www.hud.gov/grants/index.cfm> (Housing and Urban Development [HUD] Clearinghouse)
<http://www.acf.dhhs.gov/grants.html> (National Clearinghouse on Child Abuse and Neglect Information)
http://www.pswn.gov/library/lib_funding.htm (PSWN Program)

Funding Resources

<http://www.access.gpo.gov> (U.S. Government Printing Office)

<http://www.whitehouse.gov/omb/grants> (Office of Management and Budget-Grants Management)

<http://www.ntia.doc.gov> (National Telecommunications and Information Administration)

<http://www.nlectc.org/agile> (Agile—Interoperability Strategies for Public Safety)

<http://www.epgctac.com> (Electronic Proving Ground—Technology Transfer Program)

<http://it.ojp.gov> (Office of Justice Programs—Information Technology Initiatives).

Corporal Clemonds reported that DOJ's Community Oriented Policing Services program was anticipated to expand significantly and that current legislation in the Senate (Bill S. 924) had the potential to address interoperability in communications. He also suggested that the Technology Transfer Program was, and might increasingly be, a good, fast-turnaround source of current generation equipment.

Corporal Clemonds closed by saying that it was important to note the distinction between "hard" funds matching (e.g., for Local Law Enforcement Block Grants), which required 10 percent cash, as opposed to "soft" matching, in which in-kind service and/or resources could be matched based on value.

2.19 Bringing Desktop Functionality to the Field with 700 MHz Wideband Data

Ms. Pam Montanari, Radio System Manager, Pinellas County, Florida, provided a presentation on the 700 MHz Motorola SmartNet wideband data system known as the Greenhouse Project. She explained that the system consisted of 43 channels operational in 24 municipalities. She emphasized that personnel efficiency and productivity were increased due to the ability to quickly transfer fingerprints, photographs, and surveillance images over the air. She explained that Pinellas County was chosen to test the 700 MHz wideband data solution because the television spectrum was clear. Ms. Montanari further explained that the system was a partnership agreement between Pinellas County and Motorola; and it had required an initial investment of \$2 million to purchase and install the equipment for system tests.

Ms. Pam Montanari then listed the efficiency and productivity enhancements:

- Facial Recognition—improved capture and conviction
- Report Writing—rapid information sharing and increased accuracy
- Still Image Sharing—improved incident response time
- Fingerprints—positive identification
- Be on the Lookout (BOLO)—faster identification and capture or recovery
- Surveillance—reduced staffing
- Intranet Access—visual aids for responding units and increased street time.

She provided two examples of how the wideband system could be implemented in day-to-day operations. One of the examples presented by Ms. Montanari was a situation in which an officer performed a roadside check and found a container with chemicals in the trunk. The officer was not knowledgeable about hazardous materials, but was able to send real-time video of the container to a hazardous materials expert at the dispatch center. The officer was notified of what the contents were and how to handle the container.

The second example involved an outdoor crime scene in which shoeprints from the suspect were available. The officer recorded the information using video and sent it to an expert at another location. The comparison expert was able to match the evidence and provide the on-scene officer with the information.

Ms. Montanari provided a list of the Greenhouse technical highlights:

- 460 kilobits per second (Kbps) integrated voice and data, full duplex
- End-to-end IP-based packet system
- Intranet and Internet access
- VoIP (IMBE vocoder)
- Video applications (streaming video over IP)
- Quality of Service to provide special handling for voice, video, and data
- Operation on 150 kHz channel, 700 MHz FCC experimental license.

She encouraged public safety agencies to get their 700 MHz plans in place and begin the licensing process. Ms. Montanari closed by stating that high-speed data enhanced efficiency, productivity, and situational awareness for public safety personnel.

The following questions and answers were presented:

1. Do you know the approximate cost to build the backbone?
Ms. Montanari stated that she did not know the approximate cost. She did state that her group had developed a proposal to implement a three-site, three-channel, 9600 Kbps system to be implemented by 2004 at a cost of \$3 million.
2. Did you observe how range affected data throughput on the 700 MHz system?
Ms. Montanari stated that the system maintained its functionality up to 6 miles away while the designed range was only expected to be 3 miles.
3. How many of the 300 users can operate on the system at one time?
Ms. Montanari stated that more than 100 could actively be using the system at one time, and the system could have 300 to 700 inactive users on it at one time.
4. Have you performed testing with other technologies?
Ms. Montanari pointed out that she was pushing for a statewide system that would provide statewide interoperability.
5. Have you looked at your system's vulnerabilities?
Ms. Montanari explained that the 700 MHz system used 128-bit encryption and had multiple advanced software firewalls to protect against viruses.

2.20 Next Symposium State Presentation and Invitation

Captain Robert Sedita, Los Angeles County Sheriff's Department, and Battalion Chief Michael Morgan, Los Angeles County Fire Department, presented information on the interoperability status of Los Angeles County. Captain Sedita spoke of the issues Los Angeles

County faced with regard to consistent natural disasters and the strong need for interoperability between public safety agencies in this area. Chief Morgan went on to explain that five other counties surrounded Los Angeles County, with a population of approximately five million people, and that the Universal Studios area was one of the greatest interoperability challenges. He added that a long-term study had been completed to rebuild the entire system at a cost of \$505 million. This would be built out on a county-shared basis once the decision makers at the top level of county government were educated about the communications needs.

Both Captain Sedita and Chief Morgan encouraged all those present to attend the Los Angeles Symposium scheduled for January 28–30, 2003.