Funding of Public Safety Wireless Communications Systems

Report of the Interagency Working Group

Department of Justice
The Department of the Treasury
Department of Commerce
Federal Law Enforcement Wireless Users Group

June 1998

PREFACE

The National Performance Review (NPR) *Access America* report includes an action item that calls for the Departments of Justice, the Treasury, and Commerce, and the Federal Law Enforcement Wireless Users Group (FLEWUG) to establish an interagency working group to develop recommendations for innovative ways to fund public safety wireless communications systems. This report details the recommendations of that working group, as well as providing the rationale and provisions for a targeted federal funding initiative. In addition to those listed above, the following departments and agencies also participated in the working group:

- Department of Agriculture
- Department of the Interior
- Federal Communications Commission (FCC)
- Federal Emergency Management Agency (FEMA)
- Office of Management and Budget (OMB–Technical Issues)
- Public Safety Wireless Network (PSWN) Program Management Office (PMO).

It is recommended that this initiative be proposed as a part of the Department of Justice's Fiscal Year 2000 budget submission to OMB.

EXECUTIVE SUMMARY

From the first use of two-way radio in a Detroit police car in 1921, public safety agencies have benefited from the ability of wireless technology to make communications possible in the mobile environment where public safety personnel do their work. The challenge facing today's public safety agencies is to find the resources critically needed to take advantage of modern advanced radio communications, and to improve radio communications within and between agencies. This Interagency Working Group on Funding (IWGF) report describes and documents this challenge and recommends a cost-effective strategic role for the Federal Government to assist in meeting this challenge.

Major public safety incidents, such as the World Trade Center and Oklahoma City bombings, dramatically illustrate some of the deficiencies of existing public safety radio communications. In these incidents, public safety agencies responding from differing jurisdictions and levels of government were unable to establish and maintain effective communications. Because of the number of agencies, jurisdictions, and levels of government typically involved in responding to such incidents, a concerted and coordinated effort is needed to resolve these deficiencies.

The National Telecommunications and Information Administration (NTIA) and the Federal Communications Commission (FCC) created the Public Safety Wireless Advisory Committee (PSWAC) in 1995 to identify the needs of public safety communications. Since then, the Federal Government has implemented a number of other policy and legislative initiatives that address specific problems identified in the PSWAC Final Report. Although many of these problems are recognized within the public safety community, insufficient fiscal resources and inadequate planning at all levels of government have hindered progress toward improvement in public safety communications.

Pursuant to the National Performance Review (NPR), the IWGF was formed and has been meeting since January 1998. This report of the IWGF recommends a multiyear funding initiative totaling $162 million to address the fiscal and planning needs associated with public safety radio communications. This initiative includes $52 million for public safety radio communications planning grants, $10 million for technical assistance, and $100 million for demonstration projects. To implement this recommendation, the IWGF requests that the Attorney General include in the Department of Justice's Fiscal Year 2000 budget submission a request for a total of $87 million in "no year money", including $52 million for planning grants, $10 million for technical assistance, and $25 million for demonstration projects. The remaining $75 million for demonstration projects should be requested at $25 million per year for Fiscal Years 2001 through 2003. This funding initiative represents an initial step toward realizing a public safety communications environment that not only provides for the efficient use of limited resources, but also increases the personal safety of public safety service providers and the public as a whole.

The administration of this funding proposal will be the responsibility of the departments of Justice and Commerce. The planning grant program will be the responsibility of the Bureau

of Justice Assistance (BJA). The administration of the technical assistance will be the responsibility of National Institute of Justice (NIJ), in conjunction with the Public Safety Wireless Network (PSWN) program and NTIA. The administration of the demonstration projects will be the responsibility of NTIA. The goal of this funding initiative is to use the state planning process as a means to improve public safety communications at all levels of government. The technical assistance and demonstration projects will support this goal by enabling local and regional agencies to participate in the planning and development of statewide systems.

Current wireless communications technology can provide at least partial solutions to some of the wireless communications problems faced by the public safety community. Current wireless technology can enable secure communications through encryption technology, can be configured to common interoperability standards to foster communications between agencies, and can be designed to provide the reliably and flexibly to handle the increased usage experienced in emergency situations. Recently developed technology also increases the ability of diverse agencies to share a single system. Appropriate use of these shared systems can provide an elegant solution to interoperability while conserving spectrum and reducing costs.

Public safety agencies nationwide have invested an estimated $18.3 billion in land mobile radio communications systems. Upgrading and improving an infrastructure investment of this magnitude will require the combined resources of all public safety agencies at all levels of government. This report documents a clear need and substantial precedent for federal leadership, guidance, and financial assistance to improve public safety communications. This federal role, however, is limited because providing the resources required to completely address the total public safety communications funding need is beyond the practical means of the Federal Government. In addition, with tens of thousands of public safety agencies across the United States, the Federal Government could not begin to coordinate the development of improved public safety communications for each individual agency.

Recognizing these fiscal and practical constraints, the IWGF recommends an incremental, targeted, leveraged, and strategic role for the Federal Government in addressing the deficiencies of public safety communications. In the initial strategic role proposed here, the Federal Government would provide leadership and coordination in the planning and design of statewide public safety communications systems. In addition, the Federal Government would provide funding to implement public safety communications demonstration projects which address interoperability, spectrum efficiency, and system security. This proposal will allow the Federal Government to leverage its ability to improve public safety communications by ensuring that the development of statewide public safety communications systems is strategically planned and designed to improve public safety communications. Moreover, this proposal could prove a useful tool as state and local public safety agencies attempt to secure funding from within their own jurisdictions. By targeting the state level, the Federal Government provides the broadest and most efficient policy influence. Additionally, focusing on the state level provides flexibility to plan and develop public safety communications systems that meet the individual needs of all public safety agencies operating within the state.

The planning grant program recommended here will encourage states to include several criteria in their planning process, including a component to facilitate interoperability among all local, state, and federal public safety agencies operating in the state and a plan to encourage the use of spectrum efficient technologies. The program will also assist states in recognizing the security risks associated with public safety communications systems. By addressing these criteria during the planning process, national interests are advanced through a uniform awareness across the country of what is required to improve public safety communications.

The planning grant program will be flexibly structured to account for states that are at various stages of systems development. Some states have done very little advanced planning while a number of states are already in the process of procuring replacement communications systems to improve system capacity and to take advantage of new technologies. This funding initiative is strategically timed—as thousands of jurisdictions will be procuring systems over the next 5 to 10 years. Additionally, the demonstration projects will provide valuable lessons and best practices to guide other public safety agencies as they replace their public safety communications systems.

Although this report focuses on funding, all wireless communications are equally dependent on the availability of radio spectrum. Radio spectrum, a finite resource, is increasingly in demand for commercial and government purposes. Insufficient spectrum for public safety use results in communications congestion and has inhibited public safety agencies' plans to expand their systems to meet growing operational requirements. A lack of spectrum has also limited public safety agencies' ability to take advantage of new data transmission technologies, such as those that transmit mugshots and fingerprints for police, maps and building plans for firefighters, or x-rays and electrocardiograms for emergency medical services. Additional spectrum, therefore, should be reallocated to public safety. Equally important, however, is the need for government entities to plan, design, and build communications systems that efficiently use the currently available radio spectrum. The Federal Government has an interest in ensuring that the efficient use of this limited resource is an integral part of the planning process for public safety communications systems.

Providing assistance to states in their planning of statewide communications systems creates the foundation for effective public safety communications for every public safety agency, regardless of the agency's size, mission, or level of government. Proper planning for, and implementation of, modern advanced wireless communications technology could mean that the Nation need never experience another crisis in which failed communications contributes to the loss of life and property or jeopardizes the safety of public safety personnel. Appropriate planning and investment, as envisioned by this grant proposal, are appropriate first steps toward this goal and, in the opinion of the IWGF, represent a justifiable and cost effective application of federal funds that will well serve the public interest of the entire country.

TABLE OF CONTENTS

PAGE

1. INTRODUCTION 1
1.1 Purpose 1
1.2 Background 1
1.3 Scope 1
1.4 Organization 2

2. THE NATURE OF THE PROBLEM 3
2.1 Lack of Public Safety Communications Interoperability 4
2.2 Insufficient Spectrum Allocated for Public Safety Use 5
2.3 Incompatible Vendor Equipment and Lack of Technology Standards 6
2.4 Inadequate System and Operational Security 7
2.5 Lack of Adequate Funding Mechanisms 8
2.6 Fiscal and Timing Attributes of the Problem 9

3. A CASE FOR FEDERAL ACTION 13
3.1 Federal Policy and Legislative Initiatives That Support Action 13
3.1.1 National Performance Review 13
3.1.2 Information Technology Management Reform Act 14
3.1.3 Security Awareness for Critical Infrastructures 15
3.1.4 Federal Role in Infrastructure Planning and Development 17
3.1.5 Congressional Actions Supporting Public Safety Communications 18
3.2 Determining a Role for Federal Government Involvement 19
3.2.1 Targeting the Early Stages of Communications System Development 20
3.2.2 Focusing on Statewide System Development 21

4. RECOMMENDATION FOR FEDERAL ACTION 23
4.1 Method for Implementing the Federal Response 23
4.2 Anticipated Results of the Federal Response 24
4.3 Accounting for States at Differing Stages of System Development 25
4.4 Administrative Conditions of the Federal Response 25

5. SUMMARY 27

Appendix A: IT04—Reengineering Through Information Technology A-1
Appendix B: A06—Access America Report B-1
Appendix C: List of Acronyms C-1

1. INTRODUCTION

1.1 Purpose

The purpose of this *Report of the Interagency Working Group on Funding (IWGF) of Public Safety Wireless Communications Systems* is to advance for budgetary consideration a federal funding initiative that will assist in achieving improved public safety wireless communications throughout the United States.[1] This response, which is called for in the National Performance Review (NPR) *Access America* report, is supported by several administration policy initiatives and legislative actions.

1.2 Background

The work of the IWGF stems from the ongoing efforts of the NPR under the leadership of the Vice President. One of the early NPR recommendations included the creation of the Government Information Technology Services (GITS) Board to provide information technology coordination for the Federal Government. In February 1997, the NPR and the GITS Board issued the *Access America* report, which included several action items to encourage and increase citizen and business access to government services. Action item six (A06) called for establishing an intergovernmental wireless public safety network. This action includes the development of a funding mechanism to improve public safety wireless communications through the creation of an interagency working group. The action called for the group to include representatives from the Department of Justice, Department of the Treasury, Department of Commerce, and the Federal Law Enforcement Wireless Users Group (FLEWUG).

The Attorney General convened this working group on January 6, 1998. In addition to the working group members cited in A06, the Attorney General invited the departments of Agriculture and the Interior, the Federal Communications Commission (FCC), the Federal Emergency Management Agency (FEMA), the Office of Management and Budget (OMB), and the Public Safety Wireless Network (PSWN) Program Management Office (PMO) to participate.

1.3 Scope

This report identifies and discusses several key issues associated with the public safety communications environment. These issues include management and coordination of public safety communications systems, spectrum management and allocation, technology standards and market competition, security, and funding. The report illustrates the need for federal funding to address planning and coordination for interoperable public safety communications systems.

[1] For the purposes of this report, public safety wireless communications does not include commercial wireless communications such as cellular or paging services.

1.4 Organization

This report is composed of an executive summary, four sections, and three appendixes.

- Section 1 provides the purpose, background, scope, and organization of the report.
- Section 2, The Nature of the Problem, describes the deficiencies of the current public safety communications environment and details the major factors contributing to the problem.
- Section 3, A Case for Federal Action, reviews the relevant federal policy and legislative initiatives that support a federal response to improve public safety communications.
- Section 4, Recommendation for Federal Action, advances a funding initiative that strategically leverages the Federal Government's ability to serve as a catalyst for planning and coordinating development of interoperable public safety communications systems.
- Section 5 provides a summary.

2. THE NATURE OF THE PROBLEM

It was a bitterly cold winter's day on January 13, 1982, in the Nation's capital. A heavy snowstorm was passing through the area creating traffic delays and school and business closures. Snow was quickly accumulating and local police and fire departments were dealing with a deluge of weather-related dispatch calls. Without warning, an Air Florida Boeing 737 filled with passengers stalled and started to descend shortly after takeoff from Washington National Airport. The aircraft struck the 14th Street Bridge and slammed into seven automobiles before plunging nose down into the partially frozen Potomac River.

Federal and local public safety agencies were dispatched immediately. Despite heavy traffic and harsh weather conditions, these agencies were quick to arrive on the scene including the Washington, DC, metropolitan police, fire, and emergency medical services departments, and a U.S. Park Police helicopter. Several survivors were located in the frozen waters of the Potomac River. Rescue efforts had to be quick, decisive, and coordinated if they were to be pulled out of the river—before they were overcome by hypothermia. However, there was a problem: Most of the agencies on the scene operated on separate radio systems that were incompatible with one another. Without the appropriate communications links, coordination among the agencies was painfully nonexistent. Frustrated with the situation, the U.S. Park Police officers lowered a life-ring from their helicopter and began pulling survivors out of the water. After pulling all but one survivor to the shoreline, the helicopter returned to the wreckage to find that the last survivor had succumbed to the icy waters. Other public safety officials on the scene focused their attention on the injuries and fatalities on the 14th Street Bridge and the major traffic tie-ups that the disaster had created. Interagency coordination was accomplished through use of telephone lines, couriers on foot, and in some instances, hand signals.

Public safety personnel were coping as best they could under the circumstances when disaster struck again—a Metrorail commuter train derailed within a subway tunnel. Preliminary reports of the incident suggested that there were numerous injuries and several fatalities. Because of the number of public safety agencies involved with the two disasters, the two single mutual aid channels set aside by local agencies became overwhelmed and unusable. Additionally, intra-agency coordination became increasingly difficult because of the amount of radio traffic present on all channels. With lives at stake in both accidents, intra-agency radio communications were actually hindering the rescue efforts.

The "problem" that the users of public safety communications face is actually a series of interlaced problems that form a barrier to achieving improved public safety communications. A recurring theme in describing the cause of many of these problems is the lack of funding. As stated in the *Public Safety Wireless Advisory Committee (PSWAC) Final Report*, "congested and fragmented spectral resources, inadequate funding for technology upgrades, and a wide variety of governmental and institutional obstacles result in a critical situation which, if not addressed expeditiously, will ultimately compromise the ability of public safety officials to protect life and

property."[2] Additionally, the Vice President's NPR identified the need for alternative funding mechanisms as one of five actions needed to improve public safety communications:

- Improve the coordination of public safety wireless communications
- Provide adequate radio frequency spectrum for public safety agencies
- Support the development of technical standards for public safety wireless communications systems
- Include security in all public safety land mobile radio systems
- Establish an alternative funding mechanism for local, state, and federal public safety officials to improve their wireless communications systems.

Lack of funding was also identified in the PSWAC Final Report as one of five major problems confronting public safety communications. These factors were as follows:

- Lack of interoperability among public safety agencies
- Insufficient spectrum allocated to public safety
- Incompatible vendor equipment and a lack of technology standards
- Inadequate security awareness
- Lack of adequate funding mechanisms.

The lack of adequate funding is a contributing factor because limited fiscal resources have hindered the development of improved public safety communications systems. The nature of the public safety communications problem is further understood by identifying its fiscal and temporal dimensions. Determining the magnitude of the problem in fiscal terms and determining how pressing the problem is from a timing perspective are necessary to fully appreciate the nature of the problem.

2.1 Lack of Public Safety Communications Interoperability

Public safety communications interoperability refers to the ability of persons from two or more different public safety related entities to communicate, on demand and in real time, with one another. Establishing interoperable communications is vital to the task of supporting emergency response activities. The timely, coordinated response of public safety agencies is indispensable to the ability of those agencies to fulfill their mission of protecting the lives and property of the community. A critical factor in organizing a coordinated response is the ability to quickly and seamlessly establish interoperable communications among all the public safety agencies involved.

[2] *Public Safety Wireless Advisory Committee Final Report*, September 11, 1996, p. 2.

Despite its importance, interoperable communications has been realized on only a limited scale. For example, some police and fire departments operating within the same jurisdiction have achieved interoperable communications; however, these same departments may lack the ability to effectively communicate with other local, state, and federal public safety agencies operating in the same or adjacent jurisdictions. As another example, in 1991, the Federal Emergency Management Agency (FEMA) and the Department of Energy (DOE) embarked on a project to allocate frequencies in the new federal narrowband very high frequency (VHF) and ultra high frequency (UHF) channeling plans for mutual aid use by local, state and federal public safety agencies. This goal was realized in 1998 when the last channeling plan was finalized. Rules and procedures for implementing the 20 frequencies set aside for mutual aid use are currently under development. However, because the channeling plans do not become effective until the year 2005, no immediate relief is in sight.

In addition to the problem of insufficient fiscal resources to improve public safety communications, the following conditions have contributed to the lack of public safety communications interoperability:

- **Public Safety Spectrum Allocations.** Public safety radio communications are licensed in several frequency bands scattered across the spectrum. No single radio can span all the bands and interoperability thus requires the use of multiple radios or complicated, and at times ad hoc, patching schemes.

- **Spectrum Management Processes.** In the past, spectrum management processes allowed public safety agencies to implement communications systems that do not always promote interoperability.

- **Systems Planning.** The lack of adequate planning during systems development has sometimes inhibited interoperability even among public safety agencies operating in the same jurisdiction.

- **Vendor Incompatibilities.** Despite efforts to establish standards for public safety communications, competing vendors continue to manufacture, and public safety agencies continue to purchase, equipment that is not interoperable, sometimes even in the same frequency band. This is discussed in 2.3 below.

2.2 Insufficient Spectrum Allocated for Public Safety Use

As noted in the *PSWAC Final Report*, many public safety agencies experience channel overcrowding. When channel overcrowding occurs, public safety personnel must either wait for an open channel or identify other means to relay essential information. Channel overcrowding occurs when the amount of system usage closely approximates or exceeds the design capacity. Public safety communications systems are particularly susceptible to channel overcrowding because of the unpredictable surges in system usage during multiple or complex incidents.

Response efforts to emergency situations typically involve public safety agencies at many different levels (local, state, and federal) and with differing missions (law enforcement, fire suppression, and emergency medical service). The communications demands of critical situations involving these numerous agencies can overwhelm a system designed to handle a much smaller communications traffic load.

Because of the large number of public safety personnel operating in metropolitan areas and the limited number of channels dedicated to public safety in these areas, agencies located in metropolitan areas are especially susceptible to channel overcrowding. The communications systems of smaller public safety agencies can also be highly taxed when used to support disaster relief efforts involving numerous agencies. The following factors have been identified as contributing to the problem of channel overcrowding:

- **Available Spectrum.** The number of available channels for public safety use in most large metropolitan areas is insufficient to support the daily operations of the local public safety agencies. Regions such as the metropolitan areas of southern California are so "frequency starved" that any additional allotments of spectrum are immediately put to use to help alleviate the existing communications traffic burden. Additional spectrum is required to enable public safety agencies to perform their daily tasks effectively and safely.

- **System Life-Cycle Planning.** As was the case for interoperability, lack of foresight during the system planning and development phases has contributed to the problem of channel overcrowding. Inadequate planning for increases in staffing levels, technology advances, and changing operating conditions has exacerbated channel overcrowding. A majority of systems were planned and designed 20 to 30 years ago, when there were far fewer public safety personnel. Because wireless data and video transmission technology was not available to the public safety community in the 1960s and 1970s, the spectrum required for these technologies was not included in the design requirements of systems installed in that era. Additionally, police, fire, and EMS operations are much more complex today with the emergence of specialized response units such as advanced life support, hazardous material teams, and community-oriented policing. Systems life-cycle planning for public safety communications systems must account for these factors.

2.3 Incompatible Vendor Equipment and Lack of Technology Standards

The proliferation of wireless communications systems produced by multiple vendors that use incompatible transmission formats and protocols has created significant barriers to interoperability for the public safety community. A lack of standard interfaces between these incompatible formats and protocols further contributes to a lack of interoperability. This problem has led to situations where, within the same city, one agency cannot communicate with another agency even if the agencies' systems operate within the same frequency bands.

Without technical standards, commercial vendors are producing "closed systems." Many of the system infrastructure components, including mobile radios, portable radios, and base stations, are not interchangeable across vendors, and achieving interoperability among systems from different vendors generally requires unique technical solutions. To alleviate these problems, commercial vendors will need to engage in the existing standards development process. This process should address difficult issues such as sharing proprietary information and developing standards that improve interoperability and market competition.

The standards process currently under way—TIA 102/Project 25—is a joint effort of the Association of Public Safety Communications Officials, International (APCO), the National Association of State Telecommunications Directors (NASTD), agencies of the Federal Government, and the Telecommunications Industry Association (TIA). The four key objectives of this process are as follows:

- Provide enhanced functionality with equipment and capabilities focused on public safety needs
- Improve spectrum efficiency
- Ensure competition among multiple vendors through open systems architecture
- Allow effective, efficient, and reliable interagency and intra-agency communications.

In August 1995, the first phase of this two-phased standards development process was completed, and the resulting report defined most, but not all, the specifications for a complete migration to an interoperable standard. Phase II of this process, still under development, will address additional issues of voice quality, interoperability, spectrum efficiency, and multisite applications.

2.4 Inadequate System and Operational Security

The increasing reliance on computers and external resources to operate public safety communications systems has made system security an important issue in developing or upgrading communications systems. The prospect of unauthorized intrusions has created an environment in which public safety communications managers must consider security in developing and operating their communications systems. Through advances in technology, there is the potential for terrorists to interfere with public safety communications from a distant location. There have been numerous examples of unauthorized 911 system intrusions disrupting this vital service. Because many 911 systems are directly interfaced with public safety communications systems, malefactors are only one step away from disrupting public safety service by disabling or interfering with public safety communications.

Advances in communications technology, including advanced electronic scanners, decoders, and transmitters, have increased the public's ability to monitor public safety

communications. With the availability of these technologies, the well-being of public safety personnel operating in covert task forces or providing day-to-day service is compromised without the use of encryption technology or security procedures. False calls that create diversions for criminal activities and tie up several agencies at a time have been documented in areas that lack the necessary security within their systems. Thus, the lack of secure communications endangers the lives of not only public safety personnel but also the public.

The technology in existence 20 to 30 years ago was comparatively self-contained and thus isolated from intrusions. Communications systems today, however, rely on computers to control access to the system and system management. Unauthorized access to these computers can have a devastating impact on public safety service by disrupting or even disabling public safety communications. Additionally, many modern public safety communications systems rely on public phone lines to interconnect their communications network to provide more complete and efficient communications coverage. These phone lines are vulnerable to both physical and cyber intrusion. Security technology and procedures must be considered and employed to protect the components of public safety communications systems.

In summary, given changes in technology and increasing domestic terrorism, many existing public safety communications systems have inadequate security technology and procedures. Many public safety agencies are aware of their system security deficiencies; however, a lack of fiscal resources, among other factors, has precluded the implementation of technologies that would improve system security.

2.5 Lack of Adequate Funding Mechanisms

The lack of fiscal resources to replace or upgrade existing public safety communications systems has proven to be one of the largest obstacles to improving public safety communications. A lack of adequate funding has forced many public safety agencies to rely on time-consuming practices of radio swapping or ad hoc system cross patching to establish limited interoperability. These solutions, however, are short-term fixes and fail to achieve acceptable operational interoperability. In the long term, system upgrades are more cost effective, but funding constraints have inhibited such system upgrades and replacements in many cases, particularly among smaller agencies.

The notion of creating a specific revenue source to replace or upgrade these systems is not well established in the public finance and budget community. Historically, these radio systems have been fielded for 20 to 30 years, 15 to 20 years beyond their useful life cycle. The service life and significant cost of these systems lead many public finance officials to view these systems as capital assets. As capital assets, public safety communications systems must compete with other capital assets such as public buildings and road projects for limited fiscal resources. Because public safety communications systems are support systems, they are often not as visible or politically weighted as other projects such as schools or prisons, and many times are relegated to a lower funding priority.

Fiscal constraints have forced some public safety agencies to rely on alternative means to improve their communications. These alternatives include shared system development with other public and private entities and use of intergovernmental grants to improve public safety communications. However, these alternatives are not equally available to every public safety agency. Because of the significant cost of these systems, adequate and appropriate funding mechanisms must be developed for use by all public safety agencies.

2.6 Fiscal and Timing Attributes of the Problem

Combined, the factors discussed in the previous sections provide a detailed portrait of some of the key problems facing public safety communications. However, to fully appreciate the nature of these problems, financial and timing attributes must be examined.

Although public safety communications systems are not as visible as a city hall, a courthouse, or a public school, these systems represent a sizable investment in a capital infrastructure. The combined nationwide investment in the public safety communications infrastructure is significant. Quantifying the value of this investment is necessary to estimate the fiscal magnitude of the public safety communications problem.

Local governments operate nearly 52,000 police, fire, and EMS agencies.[3] These public safety agencies range in size from a single town marshal to a large urban fire department with more than 10,000 firefighters. There are an estimated 350 public safety agencies operating at the state level. Federal organizations with public safety missions are primarily located within the departments of Justice, the Treasury, Agriculture, the Interior, and Transportation (U.S. Coast Guard), and FEMA.[4]

A study to estimate the replacement value of the public safety land mobile radio (LMR)[5] infrastructure nationwide has identified the significant investment in public safety LMR systems and thus, that the cost of upgrading and improving these systems nationwide would be extraordinary. These public safety agencies are supported by other government agencies, which, while not included in this study, rely on radio communications. These agencies include state and local governmental agencies such as departments of public works, transportation, and health.

The results of the study estimate that the 1998 replacement value of the existing public safety LMR infrastructure at all levels of government is $18.3 billion.[6] This estimate represents only equipment owned by public safety agencies. The estimate does not include operating and

---

[3] *National Directory of Law Enforcement Administrators,* National Public Safety Information Bureau, 33rd Edition, 1997 and *National Directory of Fire Chiefs and Emergency Departments,* National Public Safety Information Bureau, 7th Edition, 1998.

[4] Not included are the public safety functions within the Department of Defense, the Postal Service, and other federal agencies not traditionally considered as first responders to emergency situations.

[5] Historically, LMR has served as the sole technology for public safety communications and remains the core technology today; however, it is increasingly supplemented by technologies such as cellular and paging.

[6] *Land Mobile Radio Replacement Cost Study,* PSWN Program, June 1998.

maintenance expenses, the physical structures that house the equipment, or the personnel costs associated with operating and maintaining the equipment. This estimate represents the current condition of the public safety communications infrastructure and thus does not account for the additional costs associated with achieving interoperability, spectrum efficiency, and system security. Table 2-1 provides a breakdown, by level of government, of the estimated replacement value of the existing public safety LMR infrastructure.

Table 2-1
1998 Estimated Replacement Value of Existing
Public Safety Land Mobile Radio Infrastructure

Level of Government	Cost (in $ billions)
Local	$15.4
State	$1.7
Federal [7]	$1.2
Total	$18.3

Because of the magnitude of the fiscal impact, the combined resources of public safety agencies at all levels of government are required to improve public safety communications.

Given the magnitude of the existing investment in public safety communications systems and the number of public safety agencies, it is not surprising that there is extensive current and planned public safety communications systems procurement activity at all levels of government. As of March 1998, the PSWN PMO had identified approximately 170 public safety communications system procurements in progress. These procurements range in size and scope from the Federal Bureau of Investigation to the City of Manassas, Virginia. Ironically, this increased procurement activity has the potential effect of prolonging existing problems if interoperability and the sharing of resources are not adequately addressed during the planning, design, and procurement phases of systems development.

The increase in procurement activity is attributed to the following factors:

- Insufficient system capacity
- Inadequate system functionality
- Federal spectrum policy initiatives.

The lack of sufficient attention and funding has resulted in many systems remaining in place for 20 years or more. Many public safety communications systems installed during the 1960s and 1970s reached the end of their predicted useful life cycle 10 to 15 years ago. In many cases, these legacy systems lack the capacity to support the current number of users, which is considerably more than these systems were originally designed to support. System overload and age has caused users of older systems to experience frequent congestion and disruption of

[7] Not included are the public safety functions within the Department of Defense, the Postal Service, and other federal agencies not traditionally considered as first responders to emergency situations.

service. Many of these systems cannot be expanded to accommodate additional users. Additionally, as these systems approach their full service life, they incur excessive repair and maintenance expenses. In some cases, replacement parts are no longer available for system components.

Furthermore, many legacy public safety communications systems at all levels of government cannot support modern technologies that would greatly enhance the efficiency and safety of public safety personnel. Many of these agencies are compelled to modernize their public safety communications systems both to support more efficient voice communications and also to provide the platform to support a range of current and emerging data applications.[8] These applications include computer-aided dispatch, in-vehicle report writing, and direct access to national public safety databases.

Federal policy initiatives associated with spectrum reallocation and technology standards affecting wireless communications in federal public safety agencies are also influencing procurement activity for public safety communications systems at the state and local level. Beyond replacing their public safety communications systems because of insufficient capacity and lack of functionality, state and local public safety agencies are also replacing their systems to maintain limited interoperability with federal public safety agencies. These federal policy initiatives include federal agencies vacating 235 Megahertz (MHz) of assigned spectrum that has been designated for commercial use, the migration of federal agencies to narrowband technology by the year 2005 (year 2008 for UHF band operations), and the FCC spectrum refarming initiative.

In the Omnibus Budget Reconciliation Act of 1993, Congress directed the Secretary of Commerce [i.e., National Telecommunications and Information Administration (NTIA)] to identify spectrum and develop a plan for transferring frequencies from the Federal Government to the FCC for use for emerging technologies. Consequently, in March 1995, the NTIA identified 235 MHz of federal spectrum for private sector use. In accordance with the Balanced Budget Act of 1997, NTIA recently directed the transfer of an additional 20 MHz of federal spectrum to the FCC. Along with vacating radio spectrum, the NTIA has also established a migration plan requiring all federal agencies to replace current equipment with narrowband (12.5 kHz) equipment by the year 2005. These requirements will prompt federal agencies to replace a significant portion of the federal public safety communications infrastructure. The move to narrowband technologies could potentially limit interoperability with state and local public safety agencies.

In June 1995, the FCC created a new narrowband channel plan for the private land mobile radio (PLMR) spectrum bands below 512 MHz. This plan, commonly referred to as "refarming," adopted a transition plan in which users are not required to replace existing systems; rather the transition to narrowband equipment will be managed through the FCC's "type acceptance" protocol for new radio equipment, whereby only increasingly efficient or

[8] *Draft Land Mobile Radio Procurement Report,* PSWN Program, February 1998.

narrowband equipment will be type accepted through the year 2005. Another result of the refarming initiative was the consolidation of the 20 radio service types (e.g., taxicab radio service, highway maintenance radio service, and fire radio service) into two frequency pools: public safety and industrial/business. This consolidation of radio service types will allow public safety agencies some flexibility in obtaining additional frequencies and may result in these agencies replacing existing systems as a migration to other portions of the radio spectrum designated as "public safety." For example, if frequencies are available within the portion of the radio spectrum designated as forestry-conservation radio service within the public safety frequency pool, an EMS department could apply for the use of these frequencies.

The move toward narrowband technology and the FCC refarming initiative present significant opportunities as well as challenges to the solution of the interoperability problem for local, state, and federal public safety agencies. The critical timing of the fast moving developments, and the significant investment decisions affecting public safety communications systems that are being made every day, add an urgent dimension to the communications problem that prompts a timely and targeted response.

Any one organization or any one level of government cannot address the problems contributing to the current condition of public safety communications. Addressing and resolving these many factors will require leadership and coordination at the national level. The Federal Government has provided this leadership and coordination in the past and has implemented several policy and legislative initiatives that specifically support a federal leadership role in improving public safety communications.

3. A CASE FOR FEDERAL ACTION

3.1 Federal Policy and Legislative Initiatives That Support Action

In the recent era marked by government downsizing, budget reductions, and growing threats of domestic and international terrorism, the Federal Government has initiated several policy and legislative actions that support a federal role in improving public safety communications. These actions range from providing government services more efficiently and effectively to increased security awareness for the Nation's critical infrastructures.

The policy and legislative initiatives summarized in this section, combined with the Federal Government's leadership role in developing, coordinating, and securing national infrastructures, provide the nexus for federal action to improve public safety communications. The impetus for federal action draws on the individual policy and legislative intent of these initiatives, culminating in a strong rationale for federal action.

3.1.1 National Performance Review

In 1993, Vice President Gore's focus on reinventing government dramatically changed the paradigm for providing government services. His efforts to integrate successful business practices into the government environment yielded the NPR. The NPR's goals include identifying and improving Federal Government processes to provide more efficient, cost-effective, and customer-friendly government services.

Because public safety operations are considered a critical service, they were included in the NPR. During the NPR review process, several inefficiencies related to the planning and operation of local, state, and federal public safety communications systems were identified. Two NPR reports, *Reengineering Through Information Technology* and *Access America*, have recognized the need to improve the efficiency and coordination of these systems as a way to reduce excessive duplication in operations and services. Each report emphasizes the importance of federal involvement to ensure successful coordination at the national and regional level.

Reengineering Through Information Technology established the need for federal involvement in efforts to improve public safety communications. The report provides a series of initiatives for bringing the benefits of information technology (IT) to the Federal Government. One initiative, IT04, called for the establishment of a National Law Enforcement/Public Safety Network to more effectively use IT resources within the public safety community. IT04 recognized that the role of public safety is not limited to the services provided by the Federal Government. Additionally, IT04 noted that the multilevel nature of public safety communications requires effective planning and coordination across all levels of government to meet NPR objectives. (IT04 is included as Appendix A to this report.)

The *Access America* report served as a status report on NPR IT initiatives. The focus of this report was to outline steps to encourage and increase citizen and business access to the most commonly requested government services. *Access America* contained an action item, A06,

which reiterated the importance and identified additional benefits of federal involvement in improving public safety communications systems. Such involvement could include providing efficient spectrum management, developing technical standards, and assessing and recommending innovative ways for all levels of government to fund public safety communications systems. (A06 is provided as Appendix B to this report.)

In 1996, the Federal Government responded to IT04 by beginning the PSWN program. This joint program is managed through the Department of Justice and the Department of the Treasury. The PSWN program was created to plan and foster implementation of an integrated wireless and wireline network that meets the needs of the public safety user community.

3.1.2 Information Technology Management Reform Act

The NPR is an executive branch initiative intended to improve government services. Congress has also taken steps to improve the effectiveness and efficiency of government services by passing the Information Technology Management Reform Act (ITMRA) in 1996. Like the NPR, it requires federal agencies to rethink the way they view and use information technology and its applications. These applications include wireless communications systems used by federal public safety agencies.

Through ITMRA, federal agencies are given the authority and responsibility to improve mission performance and delivery of services to the public through the strategic application of IT. ITMRA also encourages a coordinated approach in implementing IT that builds on existing information technology infrastructures and best practices. These infrastructures and practices include state and local public safety communications systems. ITMRA recognizes that the benefits of a coordinated approach include lower costs, reduced risk, and improved mission performance and service delivery. The communications systems used by public safety agencies are one area of IT that can benefit from coordinated planning and implementation across all levels of government.

Several factors germane to ITMRA are beginning to change the landscape of public safety communications. The availability of digital technology is resulting in more sophisticated and interconnected wireless communications networks. Using digital technology, wireless communications systems can be designed to interconnect and interoperate across jurisdictions and levels of government in a manner similar to computer networks. Public safety communications systems are beginning to evolve from simplistic, voice-only systems to complex IT systems that have the capability to transmit and receive video, data, and still images. Although these new technological capabilities will enable public safety agencies to provide better, more enhanced solutions to pressing problems, the sheer size, cost, and complexity of these communications systems require solid planning and sound management to truly realize the full benefits.

Because wireless communications systems are increasingly computer controlled and interconnected, ITMRA provides an opportunity for federal involvement in improving public safety communications at all levels of government by applying sound IT planning to the

development of public safety communications systems. Not only will sound planning result in the more efficient use of IT resources, it will also improve public safety communications.

3.1.3 Security Awareness for Critical Infrastructures

Local, state, and federal public safety agencies are entrusted with providing vital services that maintain civil order and ensure a stable domestic environment. These vital services constitute, in whole or in part, two national infrastructures—emergency services and government services—deemed "critical" by the President in Executive Order (E.O.) 13010, *Critical Infrastructure Protection*. Because the communications systems on which public safety agencies rely are key components of these two critical infrastructures, the Federal Government has a strong interest in ensuring that their systems are protected and secured.

On July 15, 1996, as a result of terrorist incidents such as the Oklahoma City and the World Trade Center bombings, and acknowledging infrastructure vulnerabilities brought to light after the TWA Flight 800 disaster, President Clinton issued E.O. 13010. This order acknowledged that the following eight infrastructures are of such importance that their readiness, reliability, and continuity must be viewed as a matter of national security:

- Telecommunications
- Electrical power systems
- Gas and oil transportation and storage
- Banking and finance
- Transportation
- Water supply systems
- Emergency services
- Continuity of government services.

E.O. 13010 also established the President's Commission on Critical Infrastructure Protection (PCCIP) to assess the scope and nature of threats to these eight infrastructures.

Public safety agencies and the services they provide constitute part of the *emergency services* infrastructure. As emergency services providers, public safety agencies—police, fire, emergency medical services, and others—are the first responders who protect and preserve life and property. In its final report, *Critical Foundations*, the PCCIP acknowledged that "because of their key role and because time is usually of the essence in dealing with emergencies, the inability of first-responders to handle or contain an incident can be a serious vulnerability. It can greatly amplify the effect of the initial event."

As *government services* providers, public safety and other government agencies are entrusted with performing day-to-day functions that preserve the continuity of government services. These services include the administration of justice, public health functions, and other government services that maintain civil order and protect national security interests. These

services also include activities performed by public service agencies, such as a department of public works, which are so important in the recovery phase of an emergency or disaster situation.

In providing these services, public safety agencies depend on their communications systems. Public safety communications systems are *critical service enablers* that must be protected and secured. Any attack that renders these systems incapacitated for a second, for an hour, or for days can have deadly consequences.

Because of technology advances, public safety communication systems are evolving into complex and interdependent networks. Digital land mobile radio (DLMR) systems represent the future of communications for local, state, and federal public safety agencies. This evolution from stand-alone analog systems to integrated digital systems will enable greater interconnectivity, provide data and video transmission, and transform traditional public safety communications systems into large automated information systems (AIS). In large part, this evolution to AISs makes these systems vulnerable to a host of new threats, both physical and cyber.

The *physical* threats to communications infrastructures are well known and recognized. Communications interruptions, caused by a flood, earthquake, storm, or man-made threat (e.g., bomb or arson), have been a concern for some time. Moreover, the protection of network assets, such as microwave relay antennas, telecommunications switching stations, and base stations, is an established discipline. Nevertheless, as opportunities for shared public safety communications infrastructure are realized, differing agency security requirements and practices must be resolved.

The *cyber* threats are new and emerging, and just as hazardous as *physical* threats. The DLMR architectures that make automated technologies and data transfer possible may also make it more vulnerable. As the PCCIP report states: "A computer hacker, with a laptop and modem, can have just as great of an impact as a well placed bomb."[9] For example, in 1996, a teenage hacker was able to disrupt 911 emergency phone service for 11 Florida counties from a location in Sweden. By using a computer program, the hacker was able to call the 911 operator and tie up telecommunication lines in a manner that precluded disconnection. With unchecked, uncoordinated, and nonstandardized security procedures, protocols, and management, the possible entry points into such a public safety communications network could greatly multiply.

The Federal Government has a vested interest in ensuring security issues of all types (i.e., computer, personnel, physical, and administrative) are addressed. OMB Circular A-130 directs all agencies to "protect government information commensurate with the risk and management of harm that could result from the loss, misuse, or unauthorized access to or modification of such information." Although Circular A-130 applies only to federal agencies, emerging public safety communications systems will be potentially shared and accessed by all levels of government.

---

[9] Gorelick, Jamie S., United States Deputy Attorney General, "Hearing on Security in Cyberspace," Statement before the Senate Committee on Governmental Affairs, Permanent Subcommittee on Investigations, July 16, 1996, p. 6.

NPR A06 has recognized the need for security in all public safety communications systems, and the PCCIP has urged that security policies and management practices be coordinated at all levels of government and with the private sector. The Federal Government must ensure that the policies it has set forth for its systems are being implemented at the state and local levels of government. At a minimum, the identification of security requirements, the development of security policies, and the performance of a security risk assessment are necessary to verify compliance. With emerging technology and increasing domestic terrorism, the Federal Government must provide leadership and coordination to ensure public safety communications systems are developed and maintained with the appropriate security awareness.

3.1.4 Federal Role in Infrastructure Planning and Development

The Federal Government has played a decisive role in coordinating the planning and development of certain critical infrastructures. This role has included the provision of funds and the actual engineering of new technologies. Typically, the Federal Government will choose to become involved in the development of an infrastructure that benefits the entire nation and that achieves one or more of the following missions:

- Creates a uniform infrastructure system for the common good of the Nation
- Provides a backbone system for other systems to use
- Extends a critical infrastructure to high-cost, low-population density or underserved areas to achieve equitable distribution, coverage, or universal access.

An example of successful federal development and coordination of a national infrastructure is the interstate highway system. In the early 1950s, President Eisenhower advanced the concept of creating a national highway system on the federal level. The concept arose in part as a response to the endless difficulties associated with vehicular travel, such as the annual death and injury toll, the economic loss associated with detours and traffic congestion, overburdened courts dealing with highway-related suits, and the blatant inefficiency in the transportation of goods and services.

With President Eisenhower as its champion, the plan to create a national highway system as a cooperative alliance between the states and the Federal Government moved forward. Initially, many states had not wanted to divert federal funds from local needs, and others complained that the standards for creating the national highway system were too high. However, the need to create a national highway system overrode individual state interests. As part of the Federal Highway Act of 1956, the Highway Revenue Act created the Highway Trust Fund, a self-liquidating system of financing the development of national highways that would avoid debt. The Highway Trust Fund also provides revenue for primary, secondary, and urban roads that are part of the federal-aid system.

With federal oversight and revenue collection and disbursement, the interstate highway system has been a success. The system has effectively leveraged economies of scale in linking the highway systems across states to benefit the entire nation. In the absence of this federal leadership, states would have developed a patchwork of 50 diverse state highway systems, rather than a cohesive system that crosses multiple state lines and offers universal service and benefits to all citizens. Other examples of the Federal Government developing and coordinating national infrastructures and networks include the air traffic control system and electronic funds transfer system.

As exemplified by the National Highway System, the Federal Government's leadership and coordination in infrastructure development and funding have been critical in creating nationwide infrastructures that serve all the states and sectors equally, safely, and efficiently. Without this leadership and coordination, vital systems may be developed by state and local governments and multiple commercial ventures in a way that could result in an inefficient, inequitable patchwork of systems unable to serve the entire country. To date, public safety communications systems have developed into such a patchwork of systems.

Although the resources required and the sheer number of agencies involved preclude the Federal Government from providing funding to replace public safety communications systems nationwide, the Federal Government can build on its past successes in coordinating national infrastructures to improve public safety communications.

3.1.5 Congressional Actions Supporting Public Safety Communications

For the past 15 years, specific congressional activities have contributed to the goal of improving public safety communications. Recent legislative actions addressing public safety communications have focused on the need for the Federal Government to take direct action to assist in certain aspects of the problem, such as spectrum availability and allocation.

Congressional activity regarding public safety communications began in response to the Air Florida crash and Metrorail commuter train derailment in 1982. In 1983, Congress directed the FCC to "develop a plan to ensure that the present and future electromagnetic spectrum requirements of state and local public safety authorities are considered in the allocation of available spectrum."[10] Specifically, Congress directed the FCC to review the current and future requirements of public safety agencies and to consider the need for nationwide spectrum allocation.

In 1986, the FCC allocated 6 MHz of spectrum within the 800 MHz frequency band for public safety use. As a stipulation of the allocation, the FCC prohibited any use of the new frequencies until a national plan was developed to ensure efficient use of the available spectrum. To coordinate this national plan and to ensure the involvement of public safety entities, the FCC formed the National Public Safety Planning Advisory Committee (NPSPAC). Based on the

[10] *FCC Authorization Act of 1983*, H.R. Report N. 356, 98th Cong., 1st Sess. (1983).

recommendation of NPSPAC, the FCC issued a Notice of Proposed Rulemaking in May 1987 to establish service rules and technical standards for using these 800 MHz channels. Key among the NPSPAC recommendations was the need to establish five mutual aid channels to support local, state, and federal disaster management and other emergency services.

Congressional activities addressing public safety communications followed in the early 1990s with the NTIA Organization Act, providing continuing authority to NTIA as the federal spectrum manager and as the President's principal advisor on telecommunications policies pertaining to the Nation's economic and technological advancement and to the regulation of the telecommunications industry.[11] NTIA's responsibilities include increasing the efficiency and effectiveness of spectrum use by federal agencies and facilitating the introduction of new communications technologies. In 1996, the NTIA established its Public Safety Program to coordinate spectrum and telecommunications-related activities and programs within the Federal Government as they relate to public safety.

Congress again addressed public safety communications in the Balanced Budget Act of 1997 (BBA-97). BBA-97 specifically set aside spectrum for public safety. It required the FCC to reallocate 24 MHz of spectrum between 746 and 806 MHz (TV Channels 60 to 69) for public safety services.

Over the past 15 years, Congress has increasingly supported public safety communications. In recent years, this support has become more focused as evidenced by the specific designation of 24 MHz of spectrum for public safety communications. Continued congressional support for public safety communications will be required as all of the factors contributing to the public safety communications problem are addressed.

The previously noted federal policy and legislative initiatives justify federal action to improve public safety communications. This federal action is also supported by the desire to improve government services, more efficiently use information technology resources, protect critical infrastructures, and develop national infrastructures that benefit the entire nation.

3.2 Determining a Role for Federal Government Involvement

The policy initiatives and legislative actions discussed in the previous sections indicate awareness on the part of the Federal Government that public safety agencies and the communications infrastructure on which they rely are vital to the Nation's well being. They also support the conclusion that in order for public safety agencies to fulfill their mission in a safe, effective, and secure manner, federal involvement is required in improving public safety communications.

The exact nature and magnitude of the appropriate federal role in assisting in the development of modern interoperable public safety communications systems across the nation

[11] *NTIA Manual of Regulations and Procedures for Federal Radio Frequency Management,* Chapter 1 (1997).

has not yet been defined by policy makers. However, the traditional case for some form of federal assistance appears to apply here, including the need for a uniform infrastructure system, the need for national coordination and planning, and the need for assistance to achieve equitable distribution and universal access to the network.

Even in a period of economic growth and government budget surpluses, the resources required to develop these systems and the sheer number of agencies involved is daunting, and it is clear that considerable effort by all levels of government will be required to solve this problem. The greatest share of the burden for its solution rests with the public safety community, and the case for federal involvement is limited. Nevertheless, recognizing that the federal role should be incremental, carefully targeted to achieve the desired result, and leveraged where possible to provide the greatest impact at the least economic cost, this funding proposal concludes that federal action is justified.

3.2.1 Targeting the Early Stages of Communications Systems Development

As detailed in Section 2.6, the significant replacement value of the existing public safety communications infrastructure precludes a solution simply through federal fiscal response. However, the Federal Government can play a strategic role by providing guidance and coordination during the most crucial stages of systems development.

Public safety communications systems have systems life cycles similar to other physical infrastructures or information technology systems. Public safety communications systems life cycles generally include identifying a need, planning for the solution, developing a system design, issuing a request for proposals (RFP) to procure a system, installing the system, performing systems testing and acceptance, and operating and maintaining the system. Figure 2-1 illustrates these steps in their logical sequence.

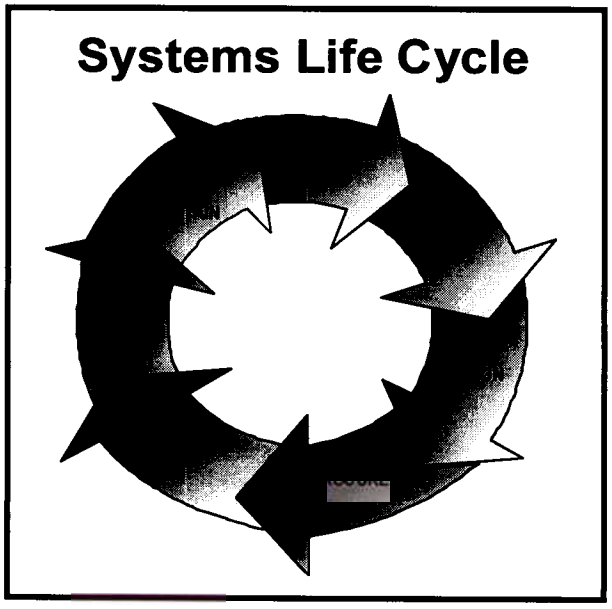

Figure 2-1

The systems life cycle construct is critical to the successful implementation of large systems such as mass transit, physical structures, and major information technology projects. Procurement and installation stages of public safety communications systems represent a small portion of the system life cycle. Measured in fiscal terms, however, the procurement and installation stages require significant financial resources. Therefore, these stages are usually funded independently of the public safety agency's operating budget.

The Federal Government can leverage its ability to provide guidance and coordination by targeting the planning and design stages for public safety communications system replacement. There is a clear need for federal involvement to ensure that the issues of interoperability are resolved in an orderly and comprehensive manner. Additionally, given rapidly changing technological advances, federal involvement is imperative over the next 5 to 10 years to provide a consistent and uniform message about what interoperability entails and to emphasize its importance to public safety agencies nationwide.

By targeting the planning and design stages, the Federal Government can provide leadership through—

- Uniform goals, relationships, and methodologies to ensure a successful implementation of an interoperable infrastructure

- Coordination of technical standards development by effectively defining requirements and recommendations for interoperable systems

- Appropriate high-level coordination that leads to the development of shared infrastructures that reduce redundancy and provide savings to public safety agencies.

3.2.2 Focusing on Statewide System Development

Improving interoperability for public safety communications is a task that must involve all levels of government. The Federal Government cannot, fiscally or administratively, begin to provide communications systems planning and design services for the tens of thousands of state and local public safety agencies. A more focused and strategic approach is required. Because of their unique position in relation to the Federal Government and local governments, state governments are in the most advantageous position to serve as the interoperability linchpin for local, state, and federal public safety agencies. Additionally, a decision to focus this initiative on the states provides the Federal Government the broadest possible policy influence with the greatest efficiency.

A given state may not, however, have a vested interest in the public safety communications concerns of individual localities or federal agencies within that state. Therefore, a state may need to be encouraged to take on the role of coordinating public safety communications interoperability among all levels of government within the state. Some financial incentive may be necessary to serve as the catalyst for action. This financial incentive,

coupled with the flexibility to develop interoperable communications systems tailored to each individual state or region, is consistent with the current federal policy of devolving the implementation of many national policy initiatives to state and local governments.

In summary, by focusing on state-level system development and targeting the planning and design stages, the Federal Government can leverage its ability to provide the greatest possible impact.

4. RECOMMENDATION FOR FEDERAL ACTION

The deficiencies in the current public safety communications environment have been well documented; federal policy and legislation to address specific aspects of these deficiencies have been initiated; and a strategic federal role to improve public safety communications has been justified. This section recommends a specific federal response and describes the anticipated results of this response. Additionally, sufficient programmatic and administrative detail is provided to serve as the basis for a federal budget initiative for the Fiscal Year 2000 budget process.

4.1 Method for Implementing the Federal Response

To encourage states[12] to coordinate the planning process for statewide public safety communications systems, the IWGF recommends a planning grant program with technical assistance, as well as funding for demonstration projects.

The funding proposal requests $162 million. This amount is based on $52 million for planning grants to the states, $10 million for technical assistance, and $100 million for demonstration projects to provide examples on how interoperability can be achieved. The technical assistance will help states understand the application of the various objectives to their individual requirements. The entire $100 million for demonstration projects is not required in the first year of the proposal. Instead, $25 million is requested for each of 4 years starting in fiscal year 2000. Thus, as states and localities move toward implementing interoperable public safety communications systems based on sound planning, there will be sufficient funding for states and localities on differing project timelines.

The proposed planning grant and technical assistance program is intended to facilitate a statewide planning process for implementing of public safety communications systems. This process will incorporate the objectives of interoperability, spectrum efficiency, and system security, and will represent the interests of all local, state, and federal public safety agencies in the state. Toward this end, the program is not intended to provide all of the necessary resources to complete a statewide plan, but only sufficient funding to ensure that the objectives are met and that all public safety agencies in the state are represented.

The demonstration projects are strategically important in providing the public safety community with examples of interoperable public safety communications systems. The results of these demonstration projects will provide valuable lessons learned and allow for the dissemination of best practices used in implementing these systems.

[12] For the purposes of this funding proposal, the term "states" includes all states and the US territories.

4.2 Anticipated Results of the Federal Response

The planning grant will encourage states to include several criteria in their plan to develop statewide public safety communications systems. At a minimum, a state plan will meet the following criteria:

- **Interoperability.** A resulting plan will provide for interoperability across all local, state, and federal public safety agencies, including American Indian and Native Alaskan Tribal Governments. Additionally, the plan will provide for an open network architecture that supports the inclusion of multiple vendors' equipment.

- **Spectrum Efficiency.** Spectrum efficiency includes technologies and management practices, such as the appropriate use of trunking, shared mutual-aid channels, and channel spacing. The plan will identify anticipated frequency and channel requirements, and catalog existing frequencies and channels of all public safety agencies in the statewide system (local, state, and federal).

- **System Coverage.** The plan must define and describe statewide operational coverage.

- **System Security.** System security includes physical and cyber security policies, equipment and training to protect the network infrastructure, and end-user equipment. In addition, the plan will specify encryption for appropriate operations.

- **Competitive Procurement.** The planning document will provide for competitive procurement, as defined by the individual state's procurement policies, of services and equipment associated with the development process.

- **Public Safety Priority Access.** The planning document must include a plan for public safety priority access to statewide systems that may include public service agencies (e.g., public works). Additionally, the plan must be able to prioritize across public safety activities. For example, one police department's routine communications should not supersede a fire department's immediate operational need.

- **Funding Analysis.** The planning document must include a funding analysis of state and local fiscal resources to determine those funds available through present and future commitments to public safety communications.

By addressing these criteria during the planning process, federal objectives are achieved through a uniform awareness of what is required to improve public safety communications.

4.3 Accounting for States at Differing Stages of System Development

Several states are already well along in developing statewide public safety communications systems. Certain of these systems, however, may not address the criteria detailed in the previous section, such as equal access by all public safety agencies and system security.

The planning grant program will be structured to account for states at differing stages of systems development. By providing some measure of flexibility in the grant program, this proposal ensures that every state stands to benefit from the program, and at the same time every state will take into account the grant program objectives.

For states that have already completed the specification and design phase of their systems, the grant award could be used to analyze these elements to ensure the grant program criteria are included. If the criteria have not been met, the grant award could be used to develop an action plan to achieve the program objectives before entering the system procurement stage.

If a state demonstrates that its system specifications and design already meet the grant program requirements, the award could be used to implement a pilot test of the system design that demonstrates interoperability with local, state, and federal public safety agencies. The desired product from the pilot testing grant award could include a detailed description of the pilot test as it relates to the system design and the grant program objectives. The product would also identify the participating agencies (local, state, and federal), the duration of the pilot test period, a summary of the lessons learned from pilot test results , and if necessary, an action plan for amending the system design.

4.4 Administrative Conditions of the Federal Response

The details of the administrative conditions and requirements will be developed during the drafting of the actual grant solicitation; however, the following administrative conditions and requirements will be included:

- **Timing**. The funding proposal will be included in the Department of Justice's Fiscal Year 2000 budget with a "no-year money" designation. In fiscal year 2000 the request would total $87 million, which includes $52 million for planning grants, $25 million for demonstration projects, and $10 million for technical assistance. In fiscal years 2001, 2002, and 2003, an additional $25 million per year (no year money) will be requested for demonstration projects.

- **Pre-approval**. The state must identify the state office, preferably within the governor's office, for fiduciary responsibility; the state agency leading the planning process; all local, state, and federal public safety agencies with wireless communications requirements operating within the state; and the method to ensure

local and federal public safety agencies are represented. The state must submit an anticipated funding plan for a statewide public safety communications system. In addition, the state must submit an anticipated budget for the planning effort. The state must submit an anticipated project timeline, both for the planning process and the overall public safety statewide communications system development.

- **Financial Management**. The grants and demonstration projects will require a 25 percent state match (either direct financial or in-kind services). The states will be reimbursed for their planning and demonstration project expenses up to the grant and project award amount based on their satisfactorily meeting the criteria detailed in the grant and project applications.

- **Procurement**. If commercial professional services are retained to assist in the planning process, the procurement of these services must be competitive, at least to the standard of the state's procurement policies. Procurement of the actual system, sub-components of the system, or professional services for project management must also be competitive, at least to the standard of the state's procurement policies.

- **Administrative Reporting**. Once awarded, quarterly updates will need to be provided, including a planning progress report, identification of authorized representatives of local and federal public safety agencies, and additional information concerning dedicated funding sources.

The administration of this funding proposal will be the responsibility of the departments of Justice and Commerce. The planning grant program will be the responsibility of the Bureau of Justice Assistance (BJA). The administration of the technical assistance will be the responsibility of National Institute of Justice (NIJ), in conjunction with the PSWN program and NTIA. The administration of the demonstration projects will be the responsibility of NTIA, in conjunction with the PSWN program.

5. SUMMARY

Just as it has taken many years to arrive at the current state of public safety communications, so will it take many years and the collaboration of all levels of government to address all of the factors needed to achieve the next level of public safety communications. As previously noted, it is clear that a considerable effort by all levels of government will be required to solve and fund the solutions of the interoperability and technological problems of public safety communications. This report details and documents a strong case for federal action in the form of targeted funding assistance to state and local public safety agencies. This assistance is conditioned upon compliance with guidelines designed to ensure the development of interoperable, spectrually efficient, and secure public safety communications systems accessible to all levels of government.

This funding proposal to provide assistance in planning and designing statewide public safety communications systems provides a critical foundation for ultimately realizing the full potential of public safety communications. This funding proposal is recommended for inclusion in the Fiscal Year 2000 Department of Justice budget submission to OMB.

APPENDIX A

IT04: REENGINEERING THROUGH INFORMATION TECHNOLOGY

IT04: ESTABLISH A NATIONAL LAW ENFORCEMENT/ PUBLIC SAFETY NETWORK

INTEGRATED COMMUNICATIONS SIMPLIFY EMERGENCY RESPONSE

Imagine this: A fire following an earthquake is devastating a large urban area in northern California. Several local, state, and federal agencies—including fire and police units, state highway units, and national guard and defense units—are rushing to the scene. Even though they come from different jurisdictions, the units coordinate easily because they share a common communications system. The fire is contained quickly, emergency services are dispatched where needed, lives are saved, and property loss is reduced as a result.

Whether they are responding to a natural or technological disaster or performing search-and-rescue or interdiction activities, federal, state, and local law enforcement and public safety workers must be able to communicate with each other effectively, efficiently, and securely. Most of this communication occurs over tactical land mobile radio systems.

However, interoperability across these different radio systems is difficult to achieve. Federal, state, and local law enforcement agencies operate in different parts of the radio spectrum. Complicating this problem is the lack of security on most systems, leaving them open to interception and monitoring. When security is applied to the radio systems—as is done with many federal radio systems—interoperability depends on having the correct encryption key to communicate.

Moreover, every federal, state, and local law enforcement agency operates separate tactical networks in every metropolitan area in the country. Often, there are several independent network control centers operating within the same federal building with no interoperation. This expensive duplication of effort prevents the use of spectrally efficient equipment and results in less-than-optimum coverage for many agencies. In addition, technical and administrative support is duplicated throughout the federal government.

NEED FOR CHANGE

Recently, the National Telecommunications and Information Administration, a part of the Department of Commerce, mandated that federal radio users begin the transition to more spectrally efficient (digital narrowband) radio systems beginning in 1995. The Federal Communications Commission is currently addressing this

same issue applicable to state and local law enforcement and public safety. The Associated Public Safety Communications Officers, Inc., is sponsoring a federal, state, local, and industry effort to develop technical standards for the next generation narrowband digital radio systems.

Over the next 10 to 15 years, all federal government radio systems will be replaced with digital technology. If this is done on an agency-by-agency basis—as was done in the past—the cost will be enormous and the same problems with interoperability will occur, resulting in costly redundancies of equipment and staffing. Current budget conditions make it critical that the federal law enforcement, public safety, and disaster response agencies coordinate the transition to digital narrowband systems. Only through a coordinated approach will cost savings be realized and the serious interoperability problems of the past be overcome.

An excellent mechanism for addressing these complex issues—and saving considerable dollars—is a shared infrastructure: a National Law Enforcement/Public Safety Wireless Network. Development of this network can be based on the efforts of two ongoing interagency initiatives.

- The Federal Law Enforcement Wireless Users Group, a joint Treasury-Justice Department initiative, was formed to plan and coordinate future shared-use wireless telecommunications systems and resources.
- The Communications Interoperability Working Group, which consists of representatives from the Department of Defense, Coast Guard, and federal law enforcement agencies, under the auspices of the Office of National Drug Control Policy, has been defining minimum baseline requirements for current, secure, interoperable federal radio systems.

These new technological advances will permit the deployment of intelligent radio systems that are feature enhanced, spectrally efficient, and secure. Interoperability will be accomplished, and the radio system can be connected to other fixed networks to improve the flow of information—e.g., fingerprints, mug shots, or criminal records to the uniformed officer or special agent on the street. A consolidated approach will result in numerous advantages in cost and quality of service.

ACTIONS

1. Formalize the Federal Law Enforcement Wireless Users Group. (1)

The Secretary of the Treasury and the Attorney General will co-sign a memorandum of understanding (MOU) to formalize the Federal Law Enforcement Wireless Users Group by April 1994. The MOU should define the charter and membership of the group, which should include—at a minimum—representation from all Justice and Treasury law enforcement agencies and bureaus, with participation from other federal, state, and local law enforcement and public safety stakeholders.

2. Establish a National Law Enforcement/ Public Safety Wireless Network for use by federal, state, and local governments. (2)

The Government Information Technology Services Working Group should issue a memorandum by July 1994 directing the Federal Law Enforcement Wireless Users Group to coordinate establishment of an intergovernmental wireless network.

The users group should work with the Office of Management and Budget, the National Telecommunications and Information Administration, the Communications Interoperability Working Group, the Federal Emergency Management Agency, and state and local entities to:

- further define costs and benefits, and develop budget strategies; and
- develop an implementation plan for the National Law Enforcement/Public

Safety Network to cover the next 10 years.

Responsibilities must be clearly defined, since the issue of which agency or activity funds and controls the network will be a point of contention. Establishment and use of the network must be handled at the highest level to avoid turf conflicts and to focus on goals, roles, methods, and relationships.

Cross References to Other NPR Accompanying Reports

Transforming Organizational Structures, ORG05: Sponsor Three or More Cross-Departmental Initiatives Addressing Common Issues or Customers.

Department of the Treasury, TRE01: Improve the Coordination and Structure of Federal Law Enforcement Agencies.

APPENDIX B

A06: ACCESS AMERICA REPORT

NATIONAL PERFORMANCE REVIEW
AL GORE
Vice President of the United States

A06:
ESTABLISH THE INTERGOVERNMENTAL WIRELESS PUBLIC SAFETY NETWORK

Imagine this: *A nervous father reports a missing child to a local 911 telephone dispatch station. A broadcast is sent over the public safety wireless communications network describing the child. The broadcast is immediately received by all local, state, and federal public safety workers in the area. A local policeman sends out a radio message to all the public safety workers warning of dangerous flooding from heavy rains in the area the child was last seen. A park ranger responds to the flood area and locates the little girl trapped on an embankment between two washed out ravines. The ranger immediately notifies the fire and rescue services, which respond in minutes. The child is returned home safely. The little girl was rescued because all relevant public safety officials were able to communicate over a common, secure, communications network.*

The September 1993 National Performance Review report recognized the need for improving public safety communications capabilities. The report highlighted the need to address key challenges, such as competition for limited radio spectrum, limited public safety budgets, and keeping pace with advances in technology. The National Performance Review recognized that if public safety agencies coordinated their efforts in developing future systems, they could conquer those challenges, greatly enhance their abilities to fight the war on crime, and save money in the process.

The National Performance Review tasked the Federal Law Enforcement Wireless Users Group (FLEWUG) to develop a plan for a future, intergovernmental, shared use, public safety wireless communications network.

In September 1996, the joint Federal Communications Commission/ National Telecommunications and Information Administration (NTIA) Public Safety Wireless Advisory Committee validated the underlying need for establishing the intergovernmental public safety wireless network. The report concluded that "unless immediate measures are taken to alleviate spectrum shortfalls and promote interoperability,

public safety agencies will not be able to adequately discharge their obligations to protect life and property in a safe, efficient, and cost effective manner."[1]

The FLEWUG has taken positive steps to develop an intergovernmental public safety wireless network. It developed a management plan that defined the goals, objectives, and actions required to develop the network.[2]

- The management plan was used to obtain Congressional support and funding for testing the concept in several locations across the country. For example, the Public Safety Wireless Network Program Management Office is working with Iowa to establish a public safety wireless communications test bed. The FLEWUG has also implemented several consolidation projects. For example, in Hawaii, all the federal, state, and local law enforcement networks throughout the islands have been consolidated into a single microwave system under Project Rainbow. The U.S. Customs Service is sharing infrastructure to improve frequency utilization and conserve resources. In New York and New Jersey, Customs is sharing the infrastructure with the Department of Housing and Urban Development; in Grand Forks, North Dakota, and New Orleans, Louisiana, with the Immigration and Naturalization Service; and nationally, with the U.S. Border Patrol. The Customs Service and the National Guard Bureau are sharing frequencies and Over-the-Air Rekeying systems to improve drug interdiction efforts. Other agencies are also finding that they can improve efficiency and save resources by sharing. In Homestead, Florida, the Federal Bureau of Investigation (FBI) is sharing its antenna site and microwave relay with the U.S. Postal Service. These cooperative efforts have also included equipment sharing. In New York, the Drug Enforcement Agency provided the U.S. Secret Service with UHF radios to use during the United Nations 50th Anniversary celebration.

NEED FOR CHANGE

Every day, local news stations report missing children, gang activities, drug wars, natural disasters, and other tragic events. People in the United States are concerned about public safety. Law enforcement and public safety workers must be provided with the best tools technology has to offer to make citizens secure in their homes and safe on their streets.

Today, critical federal, state, and local public safety communications are transmitted over tactical land mobile radio systems. Communicating across different agencies is difficult because systems have been purchased that operate in different frequencies. Most systems lack security and are open to interception and monitoring. Amateur radio enthusiasts and criminals are able to purchase scanning devices to monitor law enforcement and public safety frequencies.

In every metropolitan area of the country, federal, state, and local public safety officials operate separate tactical communications networks. In larger cities, dozens of radio antennas and

network control centers located in the same building are unable to "talk" to one another. This inefficient and expensive use of resources demands both technical and policy solutions. The FLEWUG will demonstrate a prototype narrow band (12.5 kHz channel bandwidth) conventional, digital radio system in early 1997 with many law enforcement activities in the metropolitan Washington, DC, area. The prototype equipment was developed by several vendors, with federal agencies and the State of Virginia funding the demonstration.

ACTIONS

1. ***Improve the coordination of public safety wireless communications.***

By July 1997, the President should issue an Executive Order which directs all federal agencies with a public safety mandate and federal activities supporting the public safety community to participate in the activities of the FLEWUG in developing the future Public Safety Wireless Network.

2. ***Provide adequate radio frequency spectrum for public safety agencies.***

The Government Information Technology Services (GITS) Board and the National Telecommunications and Information Administration should work with the Federal Communications Commission to outline options to balance the spectrum needs of public safety agencies with the other spectrum users. A filing should be developed and submitted to the Commission by September 1997.

By December 1997, the FLEWUG, through the GITS Board, should submit a plan to implement the recommendations in the Public Safety Wireless Advisory Committee report.

3. ***Support the development of technical standards for public safety wireless communications systems.***

Properly defined, technical standards can provide a migration path as new technology comes to the market. The government should coordinate with industry to define and develop these standards. By June 1997, the Public Safety Wireless Network Program Management Office should provide a report which defines a consolidated federal position on standards for public safety radio systems. The report should include a Common Operating Environment for current and emerging public safety land mobile radio equipment.

4. ***Include security in all public safety land mobile radio systems.***

Future public safety land mobile radio systems must be secure. Lack of appropriate security controls creates the potential for overt or inadvertent damage, manipulation, exploitation, or denial of service. By April 1997, the GITS Board should assure that government systems security experts work with the public safety community and industry to define security guidelines, standards, and conformance test procedures for public safety land mobile radio systems and equipment.

5. ***Establish an alternative funding mechanism for federal, state, and local public safety officials to improve their wireless communications systems.***

Congress has approved the use of "asset forfeiture funds" for test systems in fiscal year 1997. Asset forfeiture funds are sums of money generated by the auction of property seized by law enforcement as a result of a criminal conviction. This funding mechanism is but one innovative way to finance equipment purchases without increasing budgets.

By May 1997, the FLEWUG, the Department of the Treasury, the Department of Justice, and the Department of Commerce should establish an interagency working group to develop recommendations for other innovative ways to fund wireless public safety systems. These recommendations should be presented to the Office of Management and Budget by September 1997.

ENDNOTES

1. Final Report of the Public Safety Wireless Advisory Committee (PSWAC), September 11, 1996, page 2.

2. The Public Safety Wireless Network of the Future, Management Plan, Working Draft, 2nd Edition, October 1995.

APPENDIX C

LIST OF ACRONYMS

APPENDIX C
LIST OF ACRONYMS

APCO	Association of Public Safety Communications Officials, International
BBA	Balanced Budget Act of 1997
BJA	Bureau of Justice Assistance
DLMR	Digital Land Mobile Radio
DOE	Department of Energy
E.O.	Executive Order
EMS	Emergency Medical Services
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
FLEWUG	Federal Law Enforcement Wireless Users Group
GITS	Government Information Technology Services
IT	Information Technology
ITMRA	Information Technology Management Reform Act
IWGF	Interagency Working Group on Funding
kHz	Kilohertz
LMR	Land Mobile Radio
MHz	Megahertz
NASTD	National Association of State Telecommunications Directors
NIJ	National Institute of Justice
NPR	National Performance Review
NPSPAC	National Public Safety Planning Advisory Committee
NTIA	National Telecommunications Information Administration
OMB	Office of Management and Budget
PCCIP	President's Commission on Critical Infrastructure Protection
PLMR	Private Land Mobile Radio
PMO	Program Management Office
PSWAC	Public Safety Wireless Advisory Committee
PSWN	Public Safety Wireless Network
RFP	Request for Proposals
TIA	Telecommunications Industry Association
UHF	Ultra High Frequency
VHF	Very High Frequency