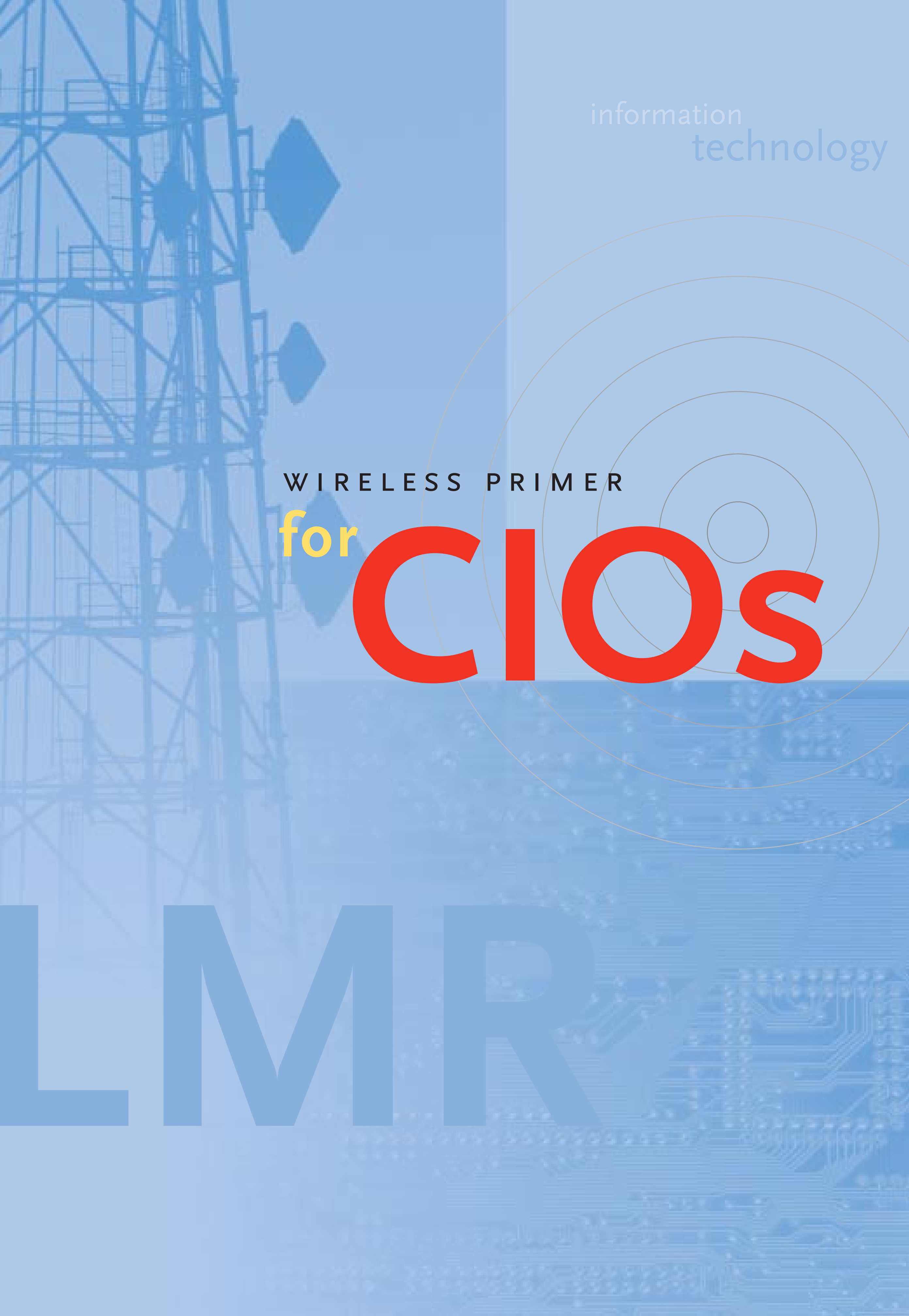
information technology

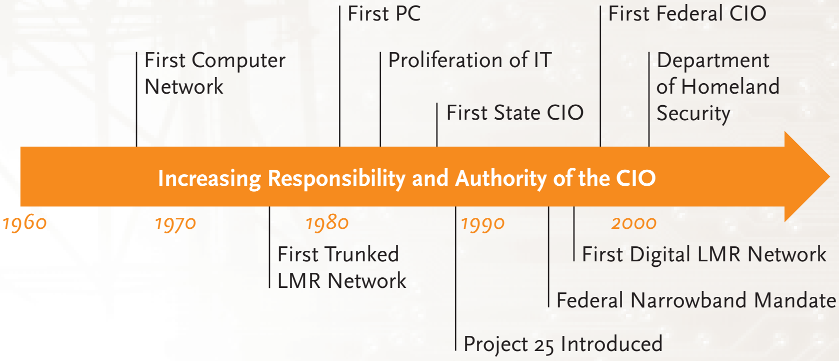
WIRELESS PRIMER for CIOs



Introduction

The information technology (IT) explosion of the 1980s and 1990s prompted local, state, and federal governments to recognize the need for chief information officers (CIO) to manage and drive governmentwide enterprise networks. Since then, these CIOs' primary concerns have been to take advantage of IT advances in order to increase work efficiency and information dissemination. Today, common CIO themes center on improving citizens' access to government services, interconnecting information systems to ensure information sharing and consistency, and protecting private information circulated electronically among citizens and government.

CIOs are often executive-level staff who report directly to the cabinet secretary (federal), governor (state), or other executive officer of the government. They are essential members of management teams, possess extensive influence and power, and have the ability to make critical decisions and effect sweeping changes. As the visibility and authority of CIOs continue to increase, the CIO role is expanding to keep up with new and broader IT functions and cross sections.


First PC
First Federal CIO
First Computer Network
Proliferation of IT
Department of Homeland Security
First State CIO
Increasing Responsibility and Authority of the CIO
1960
1970
1980
1990
2000
First Digital LMR Network
First Trunked LMR Network
Federal Narrowband Mandate
Project 25 Introduced

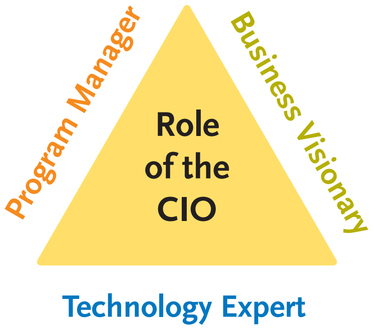
Recent homeland security initiatives have spurred a revolution in the role of the government CIO. Homeland security concerns have thrust several new IT initiatives into the realm of the CIO, addressing everything from public health to public safety. For instance, one technology not previously considered by CIOs, but increasingly gaining attention within the CIO's domain, is the wireless communications network such as land mobile radio (LMR). LMR is often used by emergency medical services (EMS), fire departments, and law enforcement personnel to communicate in a mobile environment. Most CIOs are experienced with IT projects centering on computer systems and applications but may have limited experience with wireless communications projects that often support mission critical, lifesaving operations.

The purpose of this primer is to assist CIOs who have been entrusted with the management of LMR networks in addressing potentially unfamiliar issues unique to such networks. This primer highlights some of the similarities and differences between LMR networks and traditional IT networks from the technical, programmatic, and business perspectives.

The Role of the CIO

Across the Nation, managing LMR networks is a growing responsibility for local, state, and federal CIOs. LMR networks are critical infrastructures that play a key role in maintaining our homeland security. They are large investments that require executive-level attention and leadership.

Managing LMR networks poses unique challenges unlike those associated with managing typical IT networks, such as satisfying basic public safety requirements and identifying and obtaining essential radio frequency spectrum. Consequently, managing these systems can be complex, and major pitfalls may arise when these issues are not appropriately addressed. Generally, CIOs must assume three roles when managing wireless networks—technology expert, program manager, and business visionary. The following diagram illustrates how these roles pertain to managing LMR networks.



- Architecture
- Transmission Media (Spectrum)
- Standards and Interoperability
- Security

- Funding Methods
- Strategic Planning
- Systems Lifecycle
- Outreach
- Staffing

- Long-Term Investment
- Business Case
- Market Analysis
- Procurement Arrangements

Technology Expert

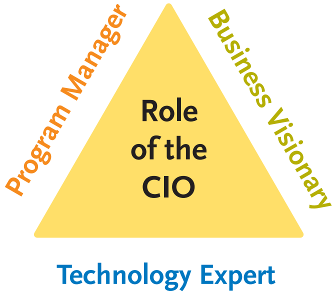
As technology experts, CIOs must be aware of the high-level technical issues that can potentially impact the successful implementation, operation, and use of their LMR networks. Many technical characteristics associated with LMR networks do not exist in typical IT networks. For instance, wireless coverage and radio frequency (RF) spectrum are basic building blocks of every LMR network.

Program Manager

Program management oversight of an LMR network requires CIOs to apply their skills and tap into strategic contacts to successfully maneuver through the LMR systems lifecycle. Although the program management approach may be similar for IT and LMR networks, the discrete tasks and manner in which the approach is executed differ due to the LMR system's high cost, long life, and distinct technical characteristics.

Business Visionary

The CIO's role as a business visionary is a relatively new responsibility. With their growing accountability for wireless networks, it is crucial that CIOs understand the market and business factors surrounding LMR technology, which differ drastically from those related to IT networks. As business visionaries, CIOs must be market savvy and be able to make critical decisions today that will yield positive returns in the near and distant future.



- Architecture
- Transmission Media (Spectrum)
- Standards and Interoperability
- Security

Technology Expert

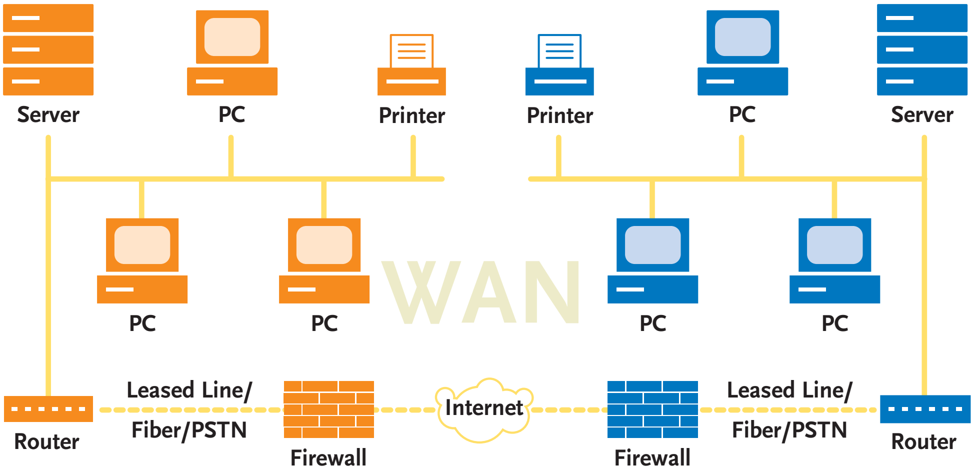
As recent as the 1980s, before the existence of the public sector CIO, individual technical experts managed most technology-related projects. As technologies advanced and IT products became more compatible, industry and government leaders quickly recognized the need to consolidate the booming IT enterprise under a single office, led by a CIO. As a result, CIOs have always been expected to maintain a broad view and understanding of many technologies.

IT advances also paved the way for the LMR industry to take advantage of microprocessors and nanotechnology, gradually transforming LMR into an offshoot of IT. Today, all modern LMR systems and networks rely heavily on IT applications, components, and architectures. Consequently, LMR technology and wireless networks are logically being included as part of CIOs' responsibility set.

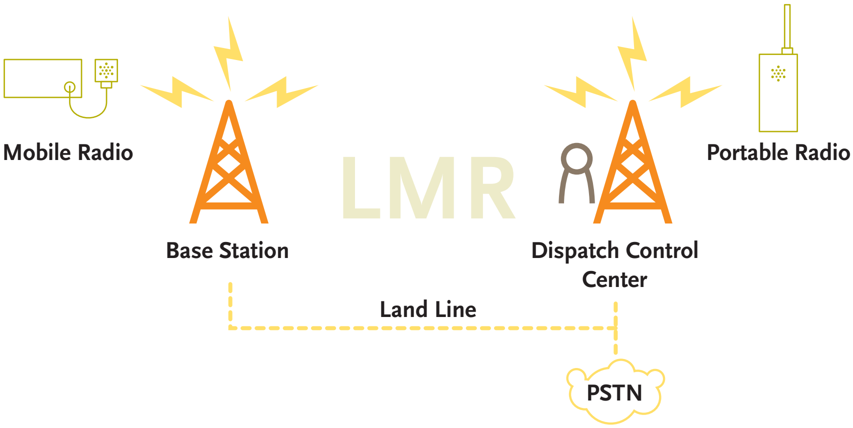
IT and LMR Networks

When discussing IT networks, this primer assumes a typical IT network is a physically wired local area network (LAN) connected to the Internet via cable, digital subscriber line (DSL), or modem. In this example, a LAN can be likened to a base station and the users within its proximity. A wide area network (WAN), which consists of multiple LANs serving a large geographic area, can be likened to an LMR network, which consists of multiple base stations serving a broad geographic area.

On the back end, WANs and LMR networks are very similar. Both rely on leased line (e.g., T1 line or fiber), land line (public switched telephone network [PSTN]), or microwave for long-haul connectivity. The "last mile" and user interface are where the two networks diverge. The following diagrams depict a typical local loop for a WAN and an LMR network.



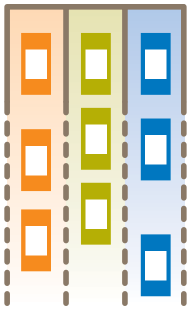
The purpose of an LMR network is to enable mobile personnel to communicate in a timely, reliable manner. Similar to WAN communications, LMR networks can also support voice, data, or video communications. These services may be provided by commercial service providers or over privately owned networks. Voice communications account for the majority of LMR transmissions, and data applications are becoming increasingly widespread. Currently, video is not commonly deployed in LMR networks because of bandwidth limitations. For simplicity, this document will focus on voice communication since it is the primary type of LMR communication.



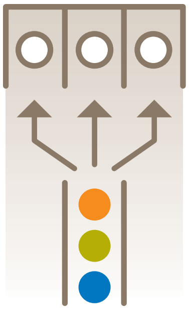
In an LMR network, the base station transmits and receives RF signals to subscriber units within its coverage area. The console gives the dispatcher a fixed interface with the network and allows simultaneous communications from a central location to numerous units. Control lines interconnect remote LMR facilities through the PSTN, leased lines, or microwave links for the purposes of communication and control. An alternative to dedicated, circuit-switched LMR networks is Internet Protocol (IP) networks. IP networks divide messages into packets that are transmitted over shared lines. IP networks offer potential cost savings through reduction or elimination of leased lines, channel equipment, and external interfaces, but they also offer varying grades of service, which can potentially impact real-time voice communications.

The basic differences between IT and LMR networks are highlighted in the following table.

Characteristic	IT	LMR
End-User Equipment	Personal computer	Handheld radio, car-mounted radio
Middleware	Routers, servers	Base stations, consoles, repeaters
Infrastructure	PSTN, leased line, microwave	PSTN, leased line, microwave
Transmission Medium	Coaxial cable, unshielded twisted pair, CAT 5, fiber optics	Radio frequency spectrum
Bandwidth	10–1000 Mbps	25 kHz/12.5 kHz (voice), 19.2 kbps (data)
Standards	HTTP, TCP/IP, PPP	Project 25
Security	Encryption, Firewall, Authentication	Encryption, Key Management, Radio Authentication, Access Controls
Useful Life	5–10 years	10–12 years
Topology/Architecture	Bus/tree, token ring, star	Conventional, trunked, hybrid



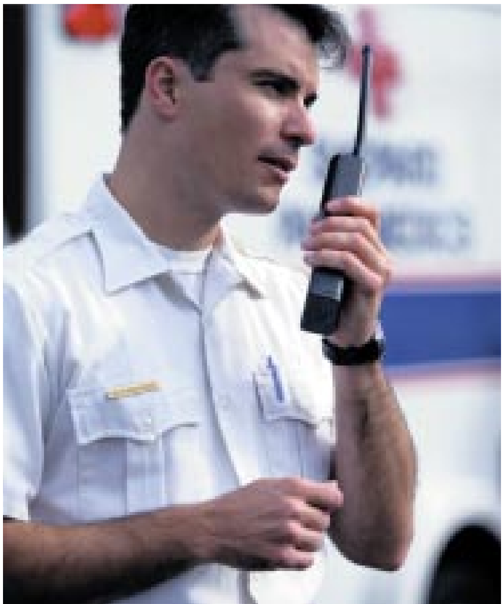
Conventional Systems
are like a tollbooth—
each user selects its own
"booth" or channel.



Trunked Systems
are like a bank line—users are
assigned a "teller" or channel based
on efficiency, priority, and location.

Conventional vs. Trunked

CIOs implementing new LMR networks need to determine the appropriate system architecture that will enable system users to satisfactorily perform their mission functions. LMR systems can be either conventional or trunked. Conventional systems are well suited for organizations with limited radio spectrum. A conventional system assigns radio channels to specific user sets. Each channel is dedicated to a specific function. Trunked systems have a greater requirement for spectrum, but make more efficient use of the spectrum. Trunked systems use access control schemes to help share a relatively small number of channels among a relatively large number of users by establishing talk groups and taking advantage of idle channels and maximizing frequency reuse. CIOs need to be aware that trunked systems cost more than conventional systems and interoperability problems often arise when users attempt to communicate between trunked and conventional systems.

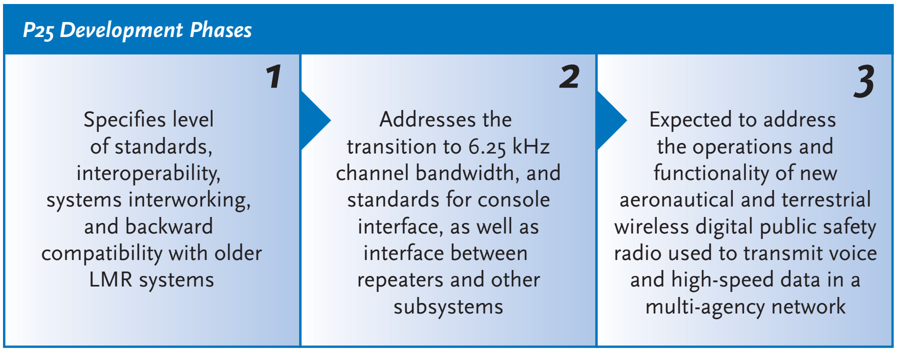


Interoperability

Market forces and government pressure sparked a massive drive to standardize computer equipment and protocols. However, CIOs managing wireless networks should not expect the same level of standardization among LMR technologies. In fact, LMR standards are not nearly as developed as IT standards. Even today, LMR technologies still exist widely as proprietary, stovepipe systems. The lack of standard technologies and protocols has been a major concern for system managers over the years. Because standards have not been fully implemented, proprietary technologies prevent organizations from effectively interoperating with each other. This is especially a concern for public safety organizations, which often need to communicate with radio users outside their home organizations or jurisdictions. To address this situation, standards-developing bodies are striving to establish uniform technical standards that pertain specifically to public safety radio communications. In the meantime, interoperability challenges are being addressed by creating policy-related and technical solutions such as console patches, crossband repeaters, audio switches, mutual-aid frequencies, and multiband, multimode radios. It is important to remember that each of these solutions is accompanied by a variety of parameters such as cost, security, and spectrum requirements that affect the selected solution.

P25 Standard

Project 25 (P25) is a suite of standards jointly developed by the public safety user community and the vendor community that addresses the development of standardized radio equipment, interoperability, spectrum efficiency, and cost economies. P25's primary objectives are twofold. First, it seeks to provide the highest performing digital, narrowband radios to meet the needs of all public safety users. Second, it looks to provide maximum interoperability among agencies and different levels of government. The following figure illustrates the three-phased development effort for the P25 suite of standards.



P25 Development Phases

1

Specifies level of standards, interoperability, systems interworking, and backward compatibility with older LMR systems

2

Addresses the transition to 6.25 kHz channel bandwidth, and standards for console interface, as well as interface between repeaters and other subsystems

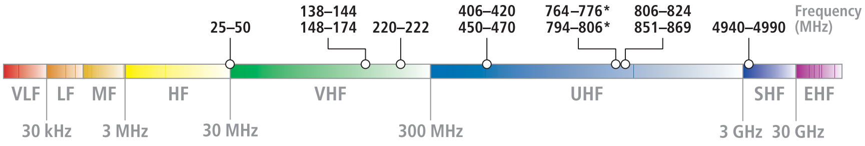
3

Expected to address the operations and functionality of new aeronautical and terrestrial wireless digital public safety radio used to transmit voice and high-speed data in a multi-agency network

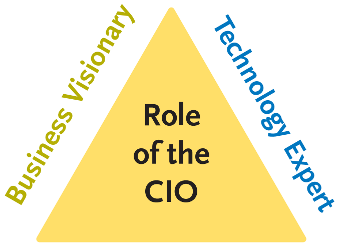
Spectrum

LMR networks, like all other wireless technologies, require radio spectrum in order to operate. Spectrum is a continuous range of frequencies with specified frequency bands used in wireless broadcasting and communications. The biggest challenge for CIOs is to manage the spectrum licensed to their organization and coordinate the sharing of this spectrum with other organizations. Federal CIOs must be aware of the narrowband mandate issued by the National Telecommunications and Information Administration (NTIA), which requires federal LMR systems operating in the very high frequency (VHF) band to be narrowbanded (i.e., use 12.5 kilohertz [kHz] channel bandwidth rather than the current 25 kHz channels) by 2006, and systems operating in the ultra high frequency (UHF) band to be narrowbanded by 2008. This requirement currently does not apply to non-federal LMR systems.

Public Safety Spectrum Bands



**Not available until 2006 or beyond*



Program Manager

- Funding Methods
- Strategic Planning
- Systems Lifecycle
- Outreach
- Staffing

Elements of a Strategic Plan:

- Introduction*
- Vision
- Mission Statement*
- Goals and Objectives*
- Strategies for Achieving Objectives*
- Relationship Between Goals and Objectives*
- Key Factors Affecting Achievement of Goals*
- Timeline
- Program Evaluation*
- Analysis and Summary of Performance Metrics

**Required of federal strategic plans*

Program Manager

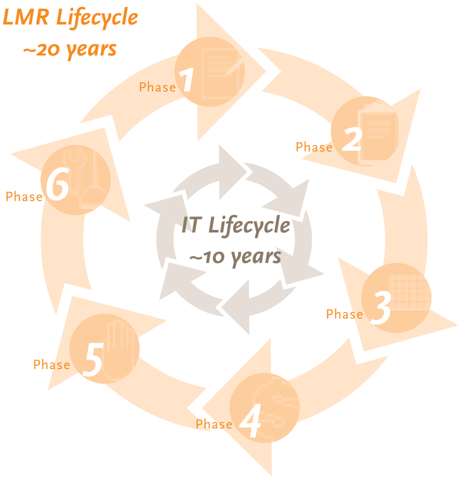
In many ways, the program management approach applied to LMR networks is very similar to that used for IT networks. Both include conducting strategic planning exercises, making formal funding requests, and performing systems lifecycle planning. The figure shows the main elements of a strategic plan that would apply to either type of network. It is noteworthy that the Office of Management and Budget (OMB) Circular A-11 requires federal agencies and departments to follow particular guidelines when developing their strategic plans. Conversely, state and local governments do not typically require strategic plans for major projects such as LMR networks, although many CIOs have developed them during the initial planning stages to help focus their vision and objectives for the project.

Lifecycle Planning

The primary factors that make management different for LMR networks are the duration of the system lifecycles, the funding levels, and the need to secure stakeholder buy-in. The following diagram depicts a typical systems lifecycle process for large-scale technical projects. The lifecycle process outlines the complete phases involved in developing and maintaining a network. It is made up of many steps including planning, procurement, and operations and maintenance. For an IT network, this entire cycle lasts about 10 years. For a LMR network, it can last upwards of 20 years. The reason for the wide gap is twofold—LMR networks last longer; therefore, they also take longer to plan, design, and implement.

Phases

1. System Planning
2. Requirements Analysis
3. Design and Engineering
4. Procurement
5. Implementation
6. Operations and Maintenance



Funding

Another primary difference between the two networks is their relative funding levels. IT projects have traditionally received more federal funding than LMR networks, often to finance high-visibility projects related to education and transportation. Recent homeland security initiatives, however, have resulted in an infusion of new federal funds geared toward improving wireless communications infrastructures, equipment, and training. CIOs should be aware of these federal grant programs and examine them carefully for restrictions, eligibility requirements, and application and award processes to determine whether their organization qualifies for a particular one. State and local CIOs should note that although their organization may qualify for some of the federal funding programs, these sources can only be expected to support a small portion of the cost of a state or local wireless network.

Stakeholders

Unlike IT initiatives, in which CIOs usually have complete authority over the outcome of the project, LMR networks are usually deployed, operated, and managed independently across government levels and jurisdictions. Although a state CIO may be responsible for a statewide LMR network, the users of the network may be local fire departments, state and local police, local EMS or, at times, federal agencies. Thus, CIOs must strike a delicate balance among all vested stakeholders—from legislators, to private citizens, to actual system users—in order to ensure successful systems lifecycle planning. As more wireless networks come under the purview of the CIO however, this level of sensitivity will be greatly mitigated.

Staffing

Finally, as with all technology networks, specialized staff is required throughout the LMR system lifecycle. The following table lists the types of staff required to plan, design, implement, and operate an LMR network.

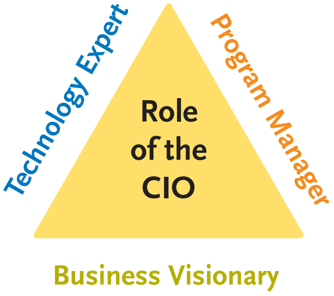
Title	Description
RF Engineer/System Planner	• Designs LMR systems • Serves as an expert on RF propagation and system components • Monitors system performance
Radio Technician	• Maintains, repairs, and installs subscriber units and radio infrastructure • Manages and maintains inventory on subscriber equipment and peripherals • Programs radios for ad hoc or planned events
Radio Manager	• Oversees the general operation of the network • Coordinates the use of backup communication systems when the primary LMR network is congested or not operational • Participates in working groups and high-level management discussions
Encryption Key Manager	• Maintains encryption keys and algorithms
Spectrum Manager/Analyst/ Frequency Coordinator	• Coordinates with regulatory bodies to obtain spectrum licenses • Informs regulatory bodies of changes or modifications in the licenses
Dispatcher	• Manages public safety responses in a service area • Sets priorities and acts on emergency and non-emergency calls for service • Establishes agency-to-agency radio interfaces and connectivity needs

Business Visionary

With their increasing role in wireless technology, CIOs must be aware of the distinct business factors surrounding LMR networks. These factors are of considerable importance because CIOs now have the responsibility and authority to make budgetary decisions, establish standards and policy, and implement change management directly associated with LMR technology. Unlike typical IT networks, LMR networks have a distinct cost structure and require rigorous strategic planning and business case analysis that take into account the system's unique return on investment. As business visionaries, CIOs should understand and be able to articulate cost outlays for LMR systems, keeping in mind that typical business measures for success do not necessarily apply when public safety is involved and lives are at stake.

Changes in LMR technology occur at a much slower rate than in IT. Therefore, the investment timeline and business approach to each technology is fundamentally different. LMR networks are typically designed to last between 10 and 12 years. However, funding challenges often force public safety agencies to operate and maintain their networks well beyond the designed useful life (at times outlasting this time frame by an additional 5 to 10 years). CIOs need to closely study the market environment and procurement arrangements for an LMR network to ensure the future availability of compatible technology, replacement parts, and maintenance services.

Business cases are required of all major federal procurements and, although not required of state agencies, state legislatures are increasingly favoring business cases to justify major investments. Business cases for LMR networks are evaluated differently from IT networks because of LMR's critical role in providing public safety services. CIOs should emphasize this fundamental difference when developing their LMR business cases to stress the long-range benefits evaluated against net present value and return on investment.



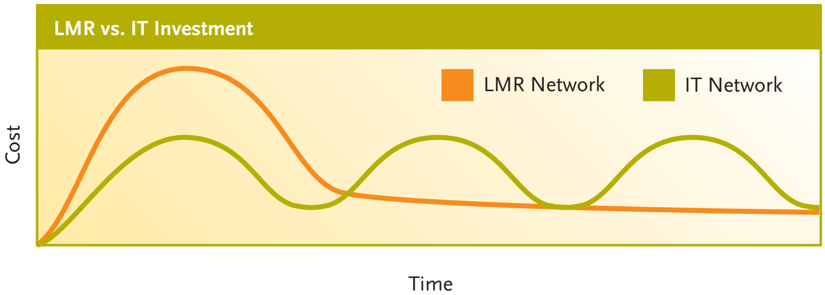
- Long-Term Investment
- Business Case
- Market Analysis
- Procurement Arrangements

LMR Market

To date, the LMR market is valued at more than $2.5 billion in annual sales, rising 16 percent annually across both analog and digital communications technologies. However, in addition to responding to new standards and regulatory requirements, the market is shifting away from analog and migrating toward digital communications systems. The analog market, currently valued at more than $1.7 billion, is decreasing in value at a rate of 7 percent per year, while the digital market, valued at $0.9 billion, is growing at a rate of 46 percent per year.

In addition, within the past few years, the LMR vendor landscape has changed considerably as a result of landmark mergers. Consequently, only a few major vendors currently serve the LMR market. Due to this increased consolidation, widespread competition is lacking and, in turn, prices are higher for both infrastructure and equipment. Therefore, it is important that CIOs and system planners perform a thorough comparative analysis of vendors' offerings to determine the most fitting infrastructure and accessories to meet the organization's funding constraints. The following table identifies primary LMR vendors and their offerings.

	Products							Target Market			
Company	Portable Radios	Mobile Radios	Desktop Radios	Trunked Architecture	Conventional Architecture	Mobile Data Applications	Command & Control Systems	Public Safety	Utility	Commercial	Military
Datron	•	•	•			•		•		•	•
EF Johnson	•	•		•	•			•		•	
Harris RF Communications	•	•									•
Kenwood Communications	•	•		•	•		•	•	•	•	
M/A-COM	•	•	•		•	•	•	•	•	•	
Motorola	•	•	•	•	•	•	•	•	•	•	•
Thales Group	•	•									•
Yaesu	•	•	•					•			



Cost Cycle

It is also important for CIOs to understand the differences in the cost timelines of LMR and IT networks. The notable difference occurs because of the differing refresh rates in end-user equipment. In general, LMR equipment has a relatively longer life than typical IT equipment. Personal, mainframe, and network computers used in IT networks average a useful life of only 2 to 3 years. Conversely, portable and mobile radios used in LMR networks can last from 5 to 7 years, depending on the degree of stress and wear and tear. Because LMR equipment is not necessarily upgraded or replaced as quickly as IT equipment, the cost trends differ sharply. This is illustrated in the figure above.

Procurement Arrangements

Like IT networks, LMR networks can be privately owned, privately leased, or commercially leased. A privately owned network wholly belongs to the organization that uses it. This option is usually favored by law enforcement agencies that have critical missions that require a high level of security, reliability, and availability. In a privately leased network, the organization usually owns the land, owns the user equipment, and holds the frequency licenses, but leases the infrastructure and major equipment from the vendor that installed the system. This arrangement usually results in the organization buying back the system from the vendor after a number of years. In a commercially leased arrangement, organizations own the user equipment, but leases everything else from the vendor, similar to cellular service arrangements. Each of the three alternatives has its relative merits, and CIOs need to weigh the pros and cons against their individual situations. Aside from these procurement arrangements, CIOs should also consider commercial wireless services such as cellular, paging, and priority access as a supplement to LMR networks. New advanced wireless data services, such as wireless broadband and and wireless fidelity (Wi-Fi),[1] are also becoming viable options for some public safety purposes due to new and improved security technologies.

[1] *For additional information on these and other advanced wireless technologies, please see the list of additional reference documents in the last section of this booklet.*

Conclusion

An unprecedented revolution has taken place in the CIO's role, responsibilities, and impact within the public sector over the past 10 years. Today, with the rapid growth in public IT investment, the increasing demand for greater efficiency in government-delivered services, and the development of technical initiatives associated with homeland security, the CIO is swiftly becoming one of the most influential positions in modern government.

In response to these revolutionary changes, CIOs across the Nation have joined together to promote a body of initiative forums. These forums serve as a focal point to coordinate concerted responses to governmentwide IT challenges and provide an opportunity for CIOs to establish partnerships with fellow executive CIOs as well as officials from other government organizations. Collectively, the CIOs can share their diverse knowledge, ideas, and best practices from their experiences with implementing wireless networks in addition to other prominent technologies.

The CIO Council

The CIO Council comprises CIOs and deputy CIOs from federal executive agencies across the Nation. The council's vision is to be a resource to help the Government work better and cost less by promoting the efficient use of agency information resources. In the area of wireless technology, addressing the issues of interoperability and secure wireless communications at all levels of the government have become two of the CIO Council's primary strategic objectives. Consequently, the CIO Council has developed a governmentwide infrastructure for fostering collaborations and sharing IT best practices, promoted the adoption of accessible technology and partnerships between the government and the wireless industry, identified standards initiatives, and developed guides that highlight implementation best practices.

NASCIO

The National Association of State Information Resource Executives (NASCIO) represents state CIOs and information resource executives and managers from 50 states, 6 U.S. territories, and the District of Columbia.

The association's vision is to shape national IT policy through collaborative partnerships, information sharing, and knowledge transfer across the jurisdictional and functional boundaries of government. NASCIO considers the improvement of wireless communications to be one of its top priorities. In concert with its own efforts, NASCIO has collaborated with prominent organizations to address the gaps in the Nation's public safety wireless communications networks to promote faster, more secure, and more reliable services. The issues NASCIO addresses include the latest technologies to promote nationwide interoperability, competitive markets, communications systems expansion, and sharing of systems to achieve efficiency.

APCO

The Association of Public-Safety Communications Officials–International, Inc. (APCO) is a nonprofit organization dedicated to promoting public safety communications. APCO's mission is to foster the development of public safety wireless communications and promote cooperation among public safety entities. The association is made up of more than 15,000 public safety users from around the world. Membership in the association comes from a myriad of organizations including law enforcement, EMS, fire, transportation, and manufacturing services.

Future Trends

Looking forward, significant changes are occurring in the wireless market that will enhance LMR technology, benefit users, and impact the role of the CIO. In addition to the creation of new standards and regulatory requirements, the LMR market is shifting away from analog systems and migrating toward digital communications systems. With this change, wireless data transmission will be possible through mobile and portable radio equipment. Capabilities such as short messaging services, enhanced telephony support, video and imagery transmission, and support for wireless LANs and WANs will soon be possible. This change will provide new capabilities and opportunities for better communications across the country in both the public and private sectors.

About the PSWN Program

The Public Safety Wireless Network (PSWN) Program is a jointly sponsored initiative of the U.S. Department of Justice and the U.S. Department of the Treasury. The PSWN Program is responsible for planning and fostering interoperability among public safety wireless networks so that local, state, federal, and tribal personnel can better communicate with each other while serving the Nation's public safety needs. Through a variety of activities, the program strives to achieve the vision it shares with the public safety community—seamless, coordinated, and integrated public safety communications for the safe, effective, and efficient protection of life and property.

The PSWN Program has developed numerous informational materials related to the topics discussed in this primer. For additional information, please refer to the following documents:

Coordination and Partnerships

- *Coordination and Partnerships Awareness Guide*
- *Role of the Local Public Safety Community in Wireless Interoperability*
- *Role of the States in Public Safety Wireless Networks*
- *Role of the Federal Government in Public Safety Wireless Networks*

Spectrum

- *Federal Spectrum Process Report*
- *State and Local Spectrum Process Report*

Funding

- *Report Card on Funding Mechanisms*
- *Public Safety Communications Funding Awareness Guide*
- *Fee-for-Service Private Wireless System Cost/Benefit Study Report*
- *How2 Guide for Funding State and Local Public Safety Wireless Networks*

Standards and Technology

- *Standards Primer*
- *Wireless Data Networking Standards Support Report*
- *How2 Guide for Managing the Radio System Life-Cycle*
- *How2 Guide for Establishing and Managing Talk Groups*
- *LMR Market Analysis Report*
- *Emerging Wireless Services Assessment*
- *Software-Enabled Wireless Interoperability Assessment Report—VoIP Technology Assessment*
- *Software-Enabled Wireless Interoperability Assessment Report—Software Defined Radio Subscriber Equipment*

Further detail regarding the PSWN Program and its products and services can be found at http://www.pswn.gov and http://www.publicsafetywins.gov. Please call the program toll free at 800.565.PSWN or contact us via e-mail at information@pswn.gov.

Acronyms

APCO	Association of Public-Safety Communications Officials-International, Inc.
CIO	Chief Information Officer
DSL	Digital Subscriber Line
EMS	Emergency Medical Service
HTTP	HyperText Transfer Protocol
IP	Internet Protocol
IT	Information Technology
kHz	Kilohertz
LAN	Local Area Network
LMR	Land Mobile Radio
Mbps	Megabits per Second
MHz	Megahertz
NASCIO	National Association of State Information Resource Executives
NTIA	National Telecommunications and Information Administration
OMB	Office of Management and Budget
P25	Project 25
PC	Personal Computer
PPP	Point-to-Point Protocol
PSTN	Public Switched Telephone Network
PSWN	Public Safety Wireless Network
RF	Radio Frequency
TCP/IP	Transmission Control Protocol/Internet Protocol
UHF	Ultra High Frequency
VHF	Very High Frequency
WAN	Wide Area Network
Wi-Fi	Wireless Fidelity

PUBLIC SAFETY
PSWN PROGRAM
WIRELESS NETWORK

www.pswn.gov

800.565.PSWN