LAW ENFORCEMENT TECH GUIDE FOR

Communications Interoperability

A Guide for Interagency Communications Projects

By Dan Hawkins

Revised and updated with contributions by Mallorie F. Teubner and Bonnie B. Maney

COPS
Community Oriented Policing Services
U.S. Department of Justice

SAFECOM

U.S. Department of Justice
Office of Community Oriented Policing Services

LAW ENFORCEMENT TECH GUIDE FOR

Communications Interoperability

A Guide for Interagency Communications Projects

By Dan Hawkins

Revised and updated with contributions by Mallorie F. Teubner and Bonnie B. Maney

The first edition of this publication was supported by cooperative agreement #2003-CK-WX-K054 awarded by the U.S. Department of Justice, Office of Community Oriented Policing Services to SEARCH Group, Incorporated, 7311 Greenhaven Drive, Suite 270, Sacramento, CA 95831. The publication was revised in 2013 under a separate cooperative agreement #2007-CK-WX-K002.The opinions or recommendations contained herein are those of the author(s) and do not necessarily represent the official position or policies of the U.S. Department of Justice. References to specific agencies, organizations, products, or services should not be considered an endorsement of the product by the author(s) or the U.S. Department of Justice. Rather, the references are illustrations to supplement discussion of the issues.

The Internet references cited in this publication were valid as of the date of this publication. Given that URLs and websites are in constant flux, neither the author(s) nor the COPS Office can vouch for their current validity.

July 2013

ISBN 978-1-935676-55-3

U.S. Department of Justice
Office of Community Oriented Policing Services
Office of the Director
145 N Street, N.E., Washington, DC 20530

COPS

Dear Colleague,

You have in your hand the revised and updated version of a guidebook that has been used by public safety first responders across the country to establish and enhance voice and data communications across jurisdictions and disciplines. The original *Law Enforcement Tech Guide for Communications Interoperability: A Guide for Interagency Communications* developed as a response to the growing concern over public safety agencies' inability to talk to each other during mission critical incidents and in daily operations that crossed jurisdictional and disciplinary lines.

From 2003–2007, the COPS Office awarded more than $400 million dollars to law enforcement agencies across the country to establish and enhance communications interoperability. During that time, we were aware of the obstacles these awardees could face if they started their journey without a guiding document to help them on their way. Thus, the *Law Enforcement Tech Guide for Communications Interoperability* was designed to meet their needs for guidance. With an endorsement from the U.S. Department of Homeland Security, we could assure our readers the guidebook was the definitive federal voice in communications interoperability guidance.

Since the Guide's first publication in 2006, our nation has undergone significant changes in the availability of communications technology and information sharing systems. In light of these changes, we determined an update of the guide was needed to provide highlights of major changes in the field. For example, the results of the SAFECOM National Interoperability Baseline Survey led to a new awareness of how far our agencies had to go to reach a basic level of interoperability. Also, the growth of NIEM (National Information Exchange Model), the introduction of statewide communications interoperability plans (SCIP), and the emergence of The National Broadband Plan and the National Emergency Communications Plan (NECP) are just some of the technological advances and policy document changes that took shape since the initial guide was released.

Developments in Communications Unit Leaders (COML) training, SAFECOM Standard Operating Procedures, and the P25 Compliance Assessment Program provided even more support to our first responders. These changes can help agencies plan and implement effective interagency communications technologies and were therefore included in the Guide's update.

Yet readers will notice that the basic premise of communications interoperability has not changed. Establishing a robust system of governance and employing project management best practices are still as relevant today as they were in 2006. These critical success factors continue to serve as the platform from which all successful interoperable communications projects can succeed. We hope that you will find this revised and updated guide helpful to you and your partners in developing an effective communications system.

Sincerely,

Bernard K. Melekian, Director
Office of Community Oriented Policing Services

Contents

Acknowledgments

This is a revised and updated version of the *Law Enforcement Tech Guide for Communications Interoperability: A Guide for Interagency Communications Projects*. The publication was prepared by SEARCH, The National Consortium for Justice Information and Statistics, Captain Thomas W. Turner, Chair, and Ronald P. Hawley, Executive Director. The project director was Scott Came, Deputy Executive Director of Programs. Mallorie F. Teubner, Director of Information Sharing Programs, and Bonnie B. Maney, Information Sharing Specialist, compiled the revisions. Twyla R. Putt, Manager, Corporate Communications, edited this publication, with assistance from Nina K. Byrom, Administrative Assistant. Debra R. Cohen McCullough, Ph.D., Senior Analyst at the U.S. Department of Justice, Office of Community Oriented Policing Services (COPS Office), was the federal project manager for the first edition and continued her work in this role, shepherding this revised and updated version through a collaborative interagency review process. Marian Haggard, Sr. Technical Editor, COPS Office, provided additional editing support. Nancy Carlsen, Sr. Graphic Designer, COPS Office, provided layout and design.

Dan Hawkins, former Director of Public Safety Programs for SEARCH, wrote the first edition in 2006. During the writing of the first edition, Francis X. (Paco) Aumand III, served as Chair, and Ronald P. Hawley, as Executive Director. The project director was Kelly J. Harris, Deputy Executive Director of Programs. Twyla R. Putt, Manager, Corporate Communications, and Linda Townsdin, Senior Writer/Editor, edited the publication. Jane L. Bassett, Publishing Specialist, provided layout and design. Chris Roebuck, Webmaster, provided website coordination.

We would especially like to acknowledge the contributions of the U.S. Department of Homeland Security's Office for Interoperability and Compatibility and the Office of Emergency Communications SAFECOM Program. The presence of the SAFECOM logo on the front cover of this Guide serves to demonstrate their support of the information offered here and use of tools created by the program, including the *Interoperability Continuum* and interoperability baseline survey.

Suggested Citation

Dan M. Hawkins, and Mallorie F. Teubner and Bonnie B. Maney (contributors), *Law Enforcement Tech Guide for Communications Interoperability: A Guide for Interagency Communications Projects*, rev. ed., Washington, D.C.: U.S. Department of Justice, Office of Community Oriented Policing Services, 2013.

About the COPS Office

The Office of Community Oriented Policing Services (COPS Office) is the component of the U.S. Department of Justice responsible for advancing the practice of community policing by the nation's state, local, territory, and tribal law enforcement agencies through information and grant resources.

Community policing is a philosophy that promotes organizational strategies that support the systematic use of partnerships and problem-solving techniques, to proactively address the immediate conditions that give rise to public safety issues such as crime, social disorder, and fear of crime.

Rather than simply responding to crimes once they have been committed, community policing concentrates on preventing crime and eliminating the atmosphere of fear it creates. Earning the trust of the community and making those individuals stakeholders in their own safety enables law enforcement to better understand and address both the needs of the community and the factors that contribute to crime.

The COPS Office awards grants to state, local, territory, and tribal law enforcement agencies to hire and train community policing professionals, acquire and deploy cutting-edge crime fighting technologies, and develop and test innovative policing strategies. COPS Office funding also provides training and technical assistance to community members and local government leaders and all levels of law enforcement. The COPS Office has produced and compiled a broad range of information resources that can help law enforcement better address specific crime and operational issues, and help community leaders better understand how to work cooperatively with their law enforcement agency to reduce crime.

- Since 1994, the COPS Office has invested nearly $14 billion to add community policing officers to the nation's streets, enhance crime fighting technology, support crime prevention initiatives, and provide training and technical assistance to help advance community policing.
- By the end of FY2012, the COPS Office has funded approximately 124,000 additional officers to more than 13,000 of the nation's 18,000 law enforcement agencies across the country in small and large jurisdictions alike.

- Nearly 700,000 law enforcement personnel, community members, and government leaders have been trained through COPS Office-funded training organizations.
- As of 2012, the COPS Office has distributed more than 8.5 million topic-specific publications, training curricula, white papers, and resource CDs.

COPS Office resources, covering a wide breadth of community policing topics—from school and campus safety to gang violence—are available, at no cost, through its online Resource Center at **www.cops.usdoj.gov.** This easy-to-navigate website is also the grant application portal, providing access to online application forms.

About SEARCH

SEARCH, The National Consortium for Justice Information and Statistics, is dedicated to improving the quality of justice and public safety through the use, management, and exchange of information; application of new technologies; and responsible law and policy, while safeguarding security and privacy.

We assist local, tribal, county, regional, and state agencies and organizations—including law enforcement and public safety; first responders; prosecution; defense; adjudication; detention; corrections and probation; and other disciplines, such as transportation, drivers' licensing, vehicle registration, public health, and social services—through a broad array of activities, resources, and products. Our focus is on criminal history systems, integrated justice information systems, information technology (planning, purchasing, managing), and cybercrime investigation. Our services include in-house and onsite technical assistance and training, resource development (websites, publications, white papers, conferences, workshops), public policy assistance, and model development (model legislation, standards and procedures, best practices) in these focus areas. SEARCH online resources provide information on law enforcement IT, integrated justice, justice software solutions, and IT acquisition at **www.search.org**.

About the Author and Contributors

DAN M. HAWKINS is a Regional Coordinator at the Department of Homeland Security, Office of Emergency Communications, where he advises federal, state, and local agencies on the subject of communications interoperability between public safety agencies. When Mr. Hawkins wrote the first edition of this publication, he was Director of Public Safety Programs for SEARCH, The National Consortium for Justice Information and Statistics, where he directed technical assistance to public safety agencies nationwide in automated systems development, planning, and integration of justice information systems, and communications interoperability.

Mr. Hawkins has 31 years of experience in the public safety field, including having been Communications Technology Manager for the State of Montana, where he managed the development of a statewide radio system. Prior to that, he served in several positions for the state, including Information Technology Operations Bureau Chief for its Department of Justice, Manager of the state's Public Safety Communications Program, and Training Officer for its Criminal Justice Information Network. He served as the FBI Information Security Officer for Montana and as adjunct faculty for both the Montana Law Enforcement Academy and Fire Services Training School. Mr. Hawkins began his public safety career as a deputy sheriff in a rural Montana county.

Mr. Hawkins is a Life Member of the Association of Public-Safety Communications Officials – International (APCO) and Associate Member of the International Association of Chiefs of Police (IACP). He has served in various roles within APCO over the years, including Chapter President, member of its International Executive Council, Chair of the Advisory Committee overseeing its frequency coordination subsidiary, and as a member of several task forces. He represented APCO on Project MESA, an international partnership developing digital mobile broadband standards worldwide, where he chaired the user committee. In 2009, he chaired the Operations Committee of a national Broadband Task Force. He currently serves on IACP's Communications and Technology Committee and previously on the Emergency Response Council of the Department of Homeland Security SAFECOM Program.

As a U.S. Forest Service-trained incident command system (ICS) Communications Unit Leader, Mr. Hawkins has served during several large law enforcement operations, wildfires, and disasters, including two large train derailments resulting in serious hazmat incidents. He worked as a lead Geographic Information Systems specialist in Colorado during the 2002 wildfire season.

Mr. Hawkins holds a bachelor's degree in Criminal Justice from Montana State University and has completed advanced management programs with the State of Montana and IBM's Advanced Business Institute. He has held basic and intermediate Peace Officer Standards and Training certificates, as well as several other certifications from the Montana Law Enforcement Academy.

MALLORIE TEUBNER is the former Director of Information Sharing Programs for SEARCH, The National Consortium for Justice Information and Statistics, where she oversaw SEARCH's initiatives to support justice and public safety information sharing nationwide. These initiatives focus on providing direct assistance to federal, state, local, and tribal practitioners with developing and executing strategies for information sharing and technology deployment. Initiatives include consulting and facilitation, strategic planning, architecture development, business process analysis, application of technology standards, and development of effective governance and funding models.

Ms. Teubner has more than 20 years of public safety experience with state and local government. For 7 years she worked for the Sangamon County (Illinois) Emergency Telephone System Department (ETSD), most recently as Director of Integrated Information Systems. In this position, she was in charge of the overall computer operations and services of the department, which provided continuous information systems support coverage for the ETSD and for more than 50 police, fire, and emergency management services agencies. For 6 years, she led and managed two government agencies as Executive Director of ETSD and the Sangamon County Central Dispatch System. This involved implementing and maintaining various technologies, including an integrated justice information system, enhanced 9-1-1, and data networks including a countywide mobile data network.

Ms. Teubner also served for 10 years with the Illinois State Police, first as a Telecommunicator and then as a business analyst in the Information Services Bureau working with multiple business partners to define requirements for statewide multiagency systems. Her law enforcement background also includes work as a Telecommunicator and 9-1-1 Operator for the Sangamon County Sheriff's Office, and as Lead Telecommunicator and Deputy Sheriff for the Pike County (Missouri) Sheriff's Department.

Ms. Teubner was a Board member of Illinois Women in Leadership, Springfield Chapter; Regional Vice President of the National Emergency Number Association (NENA), Illinois Chapter; and President of the Illinois AT&T E911 Users Group. She maintains membership in Illinois NENA and Illinois Women In Leadership, and is also a member of APCO, the Association of Public-Safety Communications Officials, International. In 2006, she received the NENA Illinois Chapter's Excellence Award, and in 1995 was selected Illinois State Police Telecommunicator of the Year.

Ms. Teubner earned a bachelor's degree, magna cum laude, in Management from the University of Illinois at Springfield. She studied Social Justice Administration and Social Work at Lincoln Land Community College in Illinois, and she attended Mineral Area College in conjunction with the Missouri Highway Patrol Academy. Ms. Teubner also has an Emergency Number Professional (ENP) certification.

BONNIE MANEY is an Information Sharing Specialist for SEARCH, the National Consortium for Justice Information and Statistics, where she helps justice and public safety agencies nationwide improve their use of technology and information sharing in mission-critical projects and initiatives. She assists in all facets of information sharing capability development and voice and data interoperability, including strategic and tactical planning, architecture development, business process modeling and analysis, service specification development, voice and data integration planning, and performance management. She also contributes to publications on key issues and participates in efforts to develop and adopt national information sharing and interoperability standards.

Ms. Maney joined SEARCH in 2010 following a 19½-year career in public safety emergency communications, most recently as Telecommunications Manager for the Town of Palm Beach (Florida) and its consolidated police/fire/emergency medical services (EMS) communications center. In that position, which she held from 2001–10, she was involved in strategic technology plan development; budget and project lifecycle management; computer-aided dispatch (CAD), radio, 9-1-1, and other communications technology; participation in policy-level stakeholder, workgroup, and user committees; analysis of user needs and requirements; and developing and administering training for operational and emergency management telecommunications and public safety personnel. Among her accomplishments was to manage communication center renovations, CAD/RMS/Radio and 9-1-1 upgrades, and other projects that enable communications interoperability and information sharing.

Before that, Ms. Maney served for 10 years as Dispatch Operations Shift Supervisor for the City of West Palm Beach, where she oversaw critical service, personnel, and equipment decisions, and performed duties of all Emergency Communications Operator positions, including call handling, police/fire/EMS dispatch, and teletype operator. She also served in the U.S. Army Reserves for 8 years, and was honorably discharged with the rank of Sergeant.

Since 2008, Ms. Maney has developed and instructed courses for the Emergency Management/Public Safety Telecommunicator degree program at Jacksonville State University (Alabama). She also has developed and instructed courses for the emergency management certificate program at Palm Beach State College (Florida) for 5 years, and also instructed in its Dispatcher Academy program. In 2012, she helped develop and present a series of online courses for the U.S. Department of Homeland Security Office of Emergency Communications on public safety communications and project management. She has also written issue briefs and best practices guides and tools on public safety broadband, ICS communications unit, interagency communications, and lifecycle management topics.

Ms. Maney earned a master's of science degree in Emergency Management from Jacksonville State University, and a bachelor's degree in Business Administration from Northwood University (Florida), where she graduated summa cum laude. She also has more than 2,000 hours of advanced training in communications, leadership, project management, equipment, and information sharing, including incident command and management systems, disaster management, and trunked and conventional radio systems, and held certification as a State of Florida 9-1-1 Emergency Dispatcher.

She is the SEARCH representative to the SAFECOM Emergency Response Council (ERC) and the First Responder Network Authority (FirstNet) Public Safety Advisory Committee (PSAC).

Review Committee

SEARCH extends its deepest thanks and appreciation to members of the *Communications Interoperability Tech Guide* Review Committee, who participated in an advisory capacity during the preparation of the first edition of this Guide.

Steve Proctor, Executive Director
Utah Communications Agency Network

John Powell, Sr., Consulting Engineer
Advanced Communications Technologies and Interoperability
U.S. Department of Homeland Security

Harlin McEwen, Chairman
Communications & Technology Committee
International Association of Chiefs of Police

Marilyn Ward, Executive Director
National Public Safety Telecommunications Council

Joe Noce, 800 MHz Project Manager
Mesa (Arizona) Police Department (Retired)

We would also like to thank members of the following agencies for contributing their time and expertise to a review of the first edition of this Guide: the Bureau of Justice Assistance and U.S. Department of Justice's (DOJ) Global Justice Information Sharing Initiative; the DOJ's Office of the Chief Information Officer; the U.S. Department of Homeland Security's (DHS) Office of Grants and Training, Preparedness Directorate; and the DHS SAFECOM Program. We are grateful to their efforts toward providing a unified federal voice to agencies across the country seeking guidance on interoperability.

Our thanks are also heartily extended to members of the following agencies who reviewed and provided feedback to this revised and updated version of this Guide: the Bureau of Justice Assistance, the DHS Office of Emergency Communications SAFECOM Program, and the National Council of Statewide Interoperability Coordinators.

A Library of Tech Guide Resources

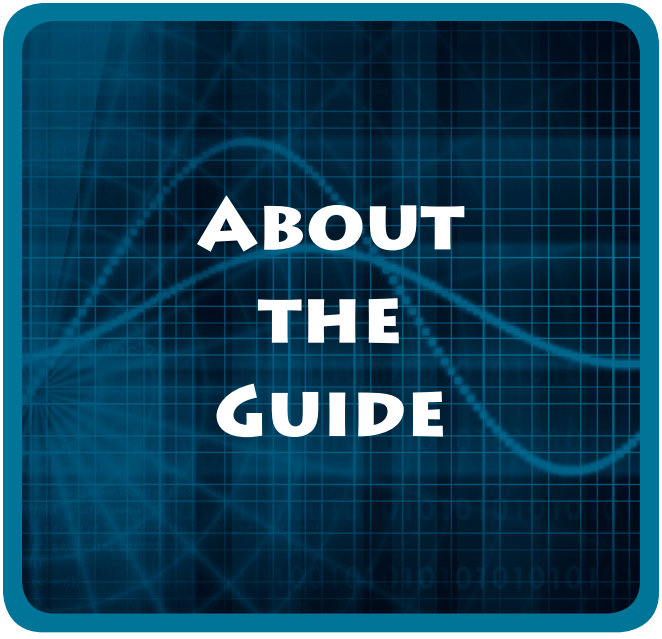
This *Tech Guide* on interoperable communications projects is intended to serve as a companion guide to the *Law Enforcement Tech Guide: How to plan, purchase and manage technology (successfully!)*. The original *Tech Guide* was published in 2002 by the U.S. Department of Justice, Office of Community Oriented Policing Services (COPS Office) and was developed as a step-by-step guide to help law enforcement agencies as they implement new technologies.

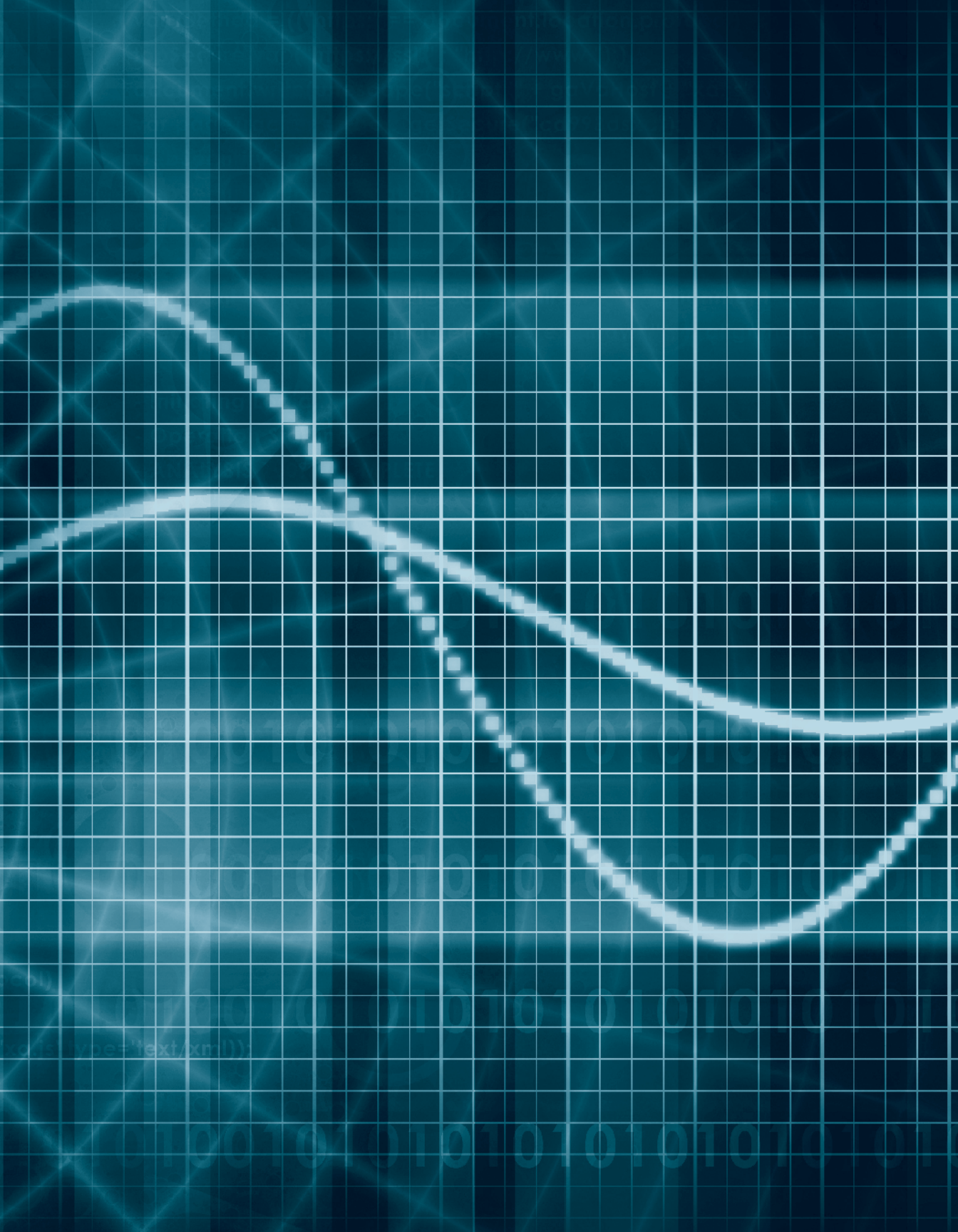
This *Communications Interoperability Tech Guide* is intended to complement and be used along with the original *Tech Guide*. As such, this Guide makes frequent references to content in the original *Tech Guide*. It may help to keep the original *Tech Guide* close at hand so you can refer to particular pages and sections as needed.

This *Tech Guide* is one of a series of four topic-specific *Tech Guides* funded by the COPS Office. These four companion *Tech Guides* form a comprehensive library of technology resources, along with the original *Tech Guide*:

- *Law Enforcement Tech Guide for Small and Rural Police Agencies: A Guide for Executives, Managers, and Technologists*
- *Law Enforcement Tech Guide for Creating Performance Measures that Work: A Guide for Executives and Managers*
- *Law Enforcement Tech Guide for Communications Interoperability: A Guide for Interagency Communications Projects*
- *Law Enforcement Tech Guide for Information Technology Security: How to Assess Risk and Establish Effective Policies*

See Page 9 for details on how to download or order your copy of the original *Tech Guide*.


About
the
Guide



COMMUNICATIONS INTEROPERABILITY IS SUCH A BIG ISSUE; how do you get your arms around the topic? Over the years the term has been used in a variety of ways to mean different things to different people. Most importantly, what does it mean to your agency and how do you approach it in a practical, systematic, and cost-effective way that best serves the public?

Well, whether you're replacing your entire radio system, replacing bits and pieces, or just looking to improve communications with other agencies without spending money, the basics are the same. *Interoperability* is built on solid foundations of leadership, cooperation, and care in understanding just what you're trying to accomplish. No amount of money can build a system allowing emergency responders across different jurisdictions to talk to each other if operational plans and procedures don't support it. **Usually we end up talking together only as well as we've planned to.**

Communications projects can be big and costly. Too often, their complexity has forced agencies to focus on internal needs without paying enough attention to *how* they will communicate with others. It's easy to fall into the trap of considering your new voice or data system to be an isolated project, unaffected by other systems that your agency and neighbors use. The result is usually a system that is integrated with the agency's other internal information and communications systems, but incapable of interoperating with cooperating neighbors.

This Guide is designed to give you, an agency executive or project manager, background on the subject of communications interoperability and tools to carry out technology initiatives that make this interoperability possible. It is intended as a companion to the *Law Enforcement Tech Guide: How to plan, purchase and manage technology (successfully!), A Guide for Executives, Managers and Technologists*.

Many references are made to the "original *Tech Guide*"; you may want to have it handy to refer to. Better yet, read it first and get an understanding of how technology projects in general are successfully carried out!

HOW TO USE THIS GUIDE

This *Communications Interoperability Tech Guide* is intended to provide background information, strategies, best practices, and recommendations for public safety communications projects. This Guide should not be construed as specific legal advice for any particular factual situation. This publication is meant to serve as a guideline for situations generally encountered in communications and information sharing planning and implementation environments. It does not replace or supersede any policies, procedures, rules, and ordinances applicable to your jurisdiction's procurement and contract negotiations. This Guide is not legal counsel and should not be interpreted as a legal service.

Assumptions…About You

This Guide is intended for staff of law enforcement or other public safety agencies who are responsible for carrying out a successful radio project. A good team is made of many players doing their own part.

If you're a chief executive of the agency, welcome aboard! Your contribution to the project is going to be critical. If you're a technical services manager, we're happy to have your expertise in both the business of your agency and how technology is aligned with its goals. Since your daily responsibility is to ensure that all systems work together, understanding the added complexities of interagency communications is vital. And if you're a technical expert who gets the calls in the middle of the night to fix the pieces that have taken an unexpected holiday, we empathize! Your interest in these systems over their lifecycles hits right at home, doesn't it?

Maybe you're the officer or communications manager who has been assigned responsibility within your agency to oversee a new voice or data system that must be compatible with other agencies you work with. Every bit of project management experience you've gathered will probably be put to work to make sure these critical and often expensive systems come together on time, within budget, and offering the capabilities everyone expects. You'll need a broad understanding of how your agency uses radio communications to provide services, how technology is chosen to support them, and why the efforts of a cross-section of people in your agency are needed to bring about a successful project.

Or maybe you're the project manager dedicated solely to this effort. If so, congratulations! Not many folks get to concentrate on a single project. More likely, your skills are valued elsewhere in the agency, too, and you have no shortage of projects on your desk.

This may be only one of several technology initiatives you're working on that demands your skills in combination with a decent understanding of the technologies involved, business practices affected, and common pitfalls others have faced.

You might think that your agency is too small or your project too tightly funded to have a full-time project manager. That certainly might be the case and if you're managing projects in such an agency, you're most likely to have other routine duties—*and* maybe even other projects. This Guide is especially useful to you because it provides a how-to guide with tips, checklists, and recommendations for your efforts—large or small!

This Guide will provide important background for all team members on how interoperability in communications systems is achieved. Its companion, the original *Law Enforcement Tech Guide*, will also be indispensable in your efforts. Get your own copy!

Assumptions…About Your Project

We assume that you already have voice radio capabilities in your agency and are either replacing systems nearing the end of their useful lives or carrying out a project to improve communications between existing systems. Maybe you're implementing a data system to augment voice communications and add new field capabilities or provide direct access to important computer systems. While this Guide doesn't address mobile data or computer systems in depth, it does address important aspects of the communications environment for both voice and data projects. Its central focus is on how to improve interagency communications across your jurisdiction.

How this Guide is Organized

This Guide is split into three parts to help you navigate to areas of greatest interest to you. Each part builds on preceding ones, but if you're in a hurry to get to work improving interagency communications, jump right to Part 2. If you're just interested in how technology is applied to achieve interoperability, Part 3 may be most useful to you.

However you approach it, please take time at some point to read the entire Guide. You will find useful background for current, as well as future, projects.

Part 1: What is Communications Interoperability?

Part 1 takes a look at what interoperability is and where we are today, as of the printing of this Guide. While we talk briefly about how and why interoperability has become a national issue, our focus is on what it means for local public safety agencies that have to talk with their neighbors.

Part 2: How is Interoperability Achieved?

Part 2 delves into how to achieve interoperability within your jurisdiction or region. It addresses steps to successful projects that were first introduced in the original *Law Enforcement Tech Guide*. The original *Tech Guide* dedicated multiple chapters to each step, so in this Guide we'll focus on additional aspects of interoperability projects or ones that require a bit more attention. The final chapter of this part takes a look at how we can measure our level of interoperability.

Part 3: Exploring the Technologies

Part 3 examines the different technological approaches to interoperability and specific types of communications equipment used in each. Since security plays an increasingly important role in public safety technology, we'll examine it with both voice and data systems.

The Guide concludes with an important appendix and fold-out with the Department of Homeland Security SAFECOM Program's *Interoperability Continuum*. This tool provides a standard set of success elements for interoperability. It also provides a snapshot of how progress is made from limited to highly interoperable public safety services. These elements are addressed from a project perspective throughout this Guide.

Our hope is to provide tools to help with your project. Icons are used in the margins as they were in the original *Law Enforcement Tech Guide*, to highlight areas of specific interest to particular project team members. Executive sponsors, for example, should keep an eye out for the shield icon shown here that is used to mark key points for project champions. Elsewhere, you will also find tips, checklists, and definitions along the way that will be useful in your quest to improve communications interoperability. In appendixes at the end of this Guide, we have included a glossary, resource materials, and sample documents.

Definition of Icons

Executive Sponsors

Executive sponsors are the project spokespersons, decision makers, and leaders of the agencies involved in the interoperability effort. Generally, they are the highest ranking decision makers within their organization. This icon is used to highlight recommendations and advice directed particularly at them.

Operational Experts

Operational experts are those communications users who understand the business processes of their respective agencies and how operations are conducted with others. Typically, these persons are senior line supervisors with experience in interagency operations. They should keep an eye out for this icon in the margins.

Technical Experts

Technical expertise is critical for analysis of the current communications technology environment and evaluation of the technical aspects of proposed solutions. This icon is used to draw attention to material that technical experts will benefit from.

Project Manager

Since the project manager has such a pivotal role, we could have used this icon on every page of the Guide. We have limited ourselves to using it to highlight aspects most commonly handled by the project manager.

Stop Sign

Every technology project is challenged to navigate in a veritable minefield of obstacles. When you see this icon, carefully read about pitfalls that we are hoping you will avoid.

Grant Requirements

This icon is used to draw your attention to interoperability aspects that may be affected by requirements of grants that may be funding your project. Even if your project is funded by other means, one of your neighbors could be relying on grants for some part of their system and you will want to learn how grant requirements are shaping *their* interagency communications plans.

Regional

Multijurisdictional, regional efforts bring the highest level of communications interoperability. This icon is used to draw your attention to advice and recommendations on how to make those efforts most successful.

Tips

This Guide is full of tips, but some need particular attention. We'll use this icon for ideas you might find immediately useful.

Checklists

We all need lists to organize a collection of thoughts or tasks. Part 2 of this Guide has a number of checklists to help you keep track of the recommendations we've provided.

Interoperability Continuum

As mentioned, the SAFECOM *Interoperability Continuum* is an important and useful tool for understanding how communications systems evolve from minimal to optimal levels of interoperability. It is included in this Guide as a back cover foldout preceded by an appendix describing its elements in depth. This icon is used to highlight those elements as they are addressed throughout the Guide.

Original ***Law Enforcement Tech Guide*** Reference

The "parent" *Law Enforcement Tech Guide: How to plan, purchase and manage technology (successfully!)*, referred throughout as the 'original *Tech Guide*' or 'original *Law Enforcement Tech Guide*,' was the first *Tech Guide* published in the *Law Enforcement Tech Guide* series. It contains many useful tools, charts, and instructions for conducting various tasks. When you see this icon, you will be directed to a specific page, or range of pages, in the original *Tech Guide*.

The U.S. Department of Justice, Office of Community Oriented Policing Services (COPS Office) published the original *Law Enforcement Tech Guide* in 2002. It is available electronically from the COPS website: **www.cops.usdoj.gov** and at SEARCH's website: **www.search.org/programs/info/publications/techguides/**.

Hard copy versions are distributed by the COPS Office. To request one, contact the COPS Office Response Center at 1-800-421-6770 or e-mail **AskCopsRC@usdoj.gov**.

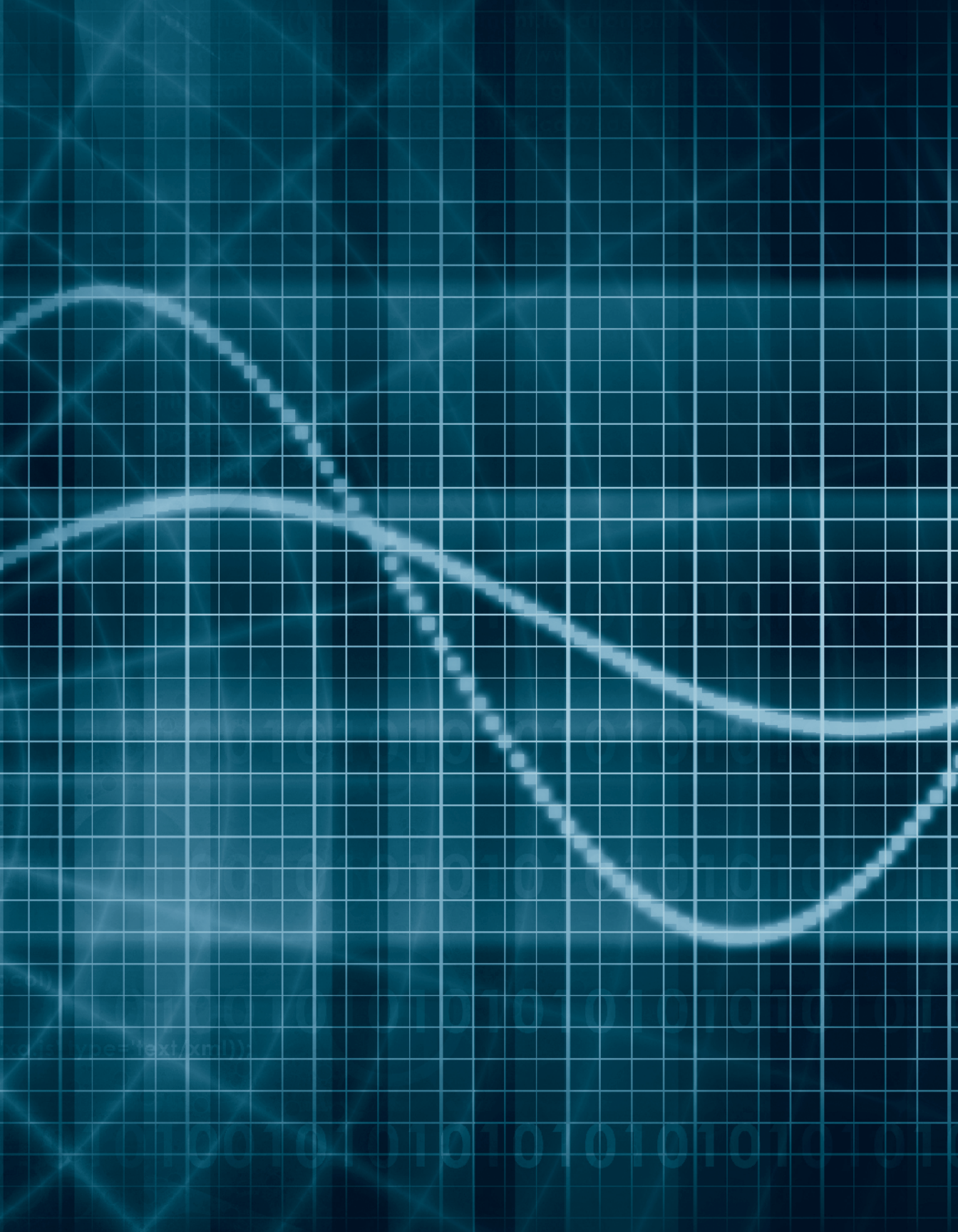
Where to Go From Here

Communications interoperability projects are technology projects. If you don't have a copy of the original *Law Enforcement Tech Guide*, download or order one. Since this Guide on interoperability is intended to complement the original, we'll often refer to it rather than repeating advice. There's a wealth of material in it about planning, purchasing, and managing technology (successfully!) that you will want to use for all sorts of projects.

If you're with a fire, emergency medical services, or other non-police agency, don't get hung up on the "Law Enforcement" part of the *Tech Guide*'s title. It was produced for that audience, but the principles and practices provided are applicable across public safety technology, generally. It has been used as a textbook by the U.S. Department of Justice and U.S. Department of Homeland Security to train dozens of jurisdictions from around the country in managing their interagency projects.

Part 1

What is Communications Interoperability?



CHAPTER 1

Introduction: A Changing Environment

IN RECENT YEARS, dramatic criminal, terrorist, and natural disasters—and seemingly endless post-incident inquiries—have seared into the public mind the importance of seamless emergency services. Today more than ever, the public expects those services will be delivered regardless of long histories of turf battles between agencies and jurisdictions. Public safety as an entity—the collective of police, fire, emergency medical services (EMS), and supporting agencies—is challenged to integrate services across these boundaries to serve a public that's not easily separated by administrative lines or simple classifications of calls.

Interoperability is the ability of agencies to work together toward common ends.

Interoperability refers to the ability of emergency responders to work seamlessly with other systems or products without any special effort. Interoperability occurs across disciplines and jurisdictions. It is expected to occur on demand, in real time, when needed, and as authorized. It is the ability of agencies to work together toward common ends.

Interoperability success depends on a common vision of what those "ends" are and how separate capabilities are combined to serve them. Most government services provided, including public safety response to emergencies, are enabled by technology. Telecommunications and information services are key enablers to effective emergency services. In recent years, public safety has recognized that interoperability goes well beyond radio communications systems. Interoperability has expanded to include other forms of communications used to relay critical information. Public safety stakeholders recognize the importance of policy development and the human resource element that makes interoperability technology work.

Communications interoperability is constantly and rapidly changing in an environment with strong public expectations, evolving communications needs, developing technologies, and a growing understanding of how all of these parts work together.

Public Expectations

What does the public expect? For the most part, the public expects effective and efficient problem solving. When Mrs. Smith calls 9-1-1, she doesn't want to hear about turf issues and technological incompatibilities. She expects services will be delivered promptly and effectively to address her emergency. No amount of explanation of jurisdictions, policies, or radio failures will matter (or be acceptable) in time of need.

The public expects that emergency responders are able to communicate with one another. Expected outcomes of that ability, in management terms, include:

- **Responder accountability –** That those brave souls who "face the elephant" aren't lost in the fog of battles.
- **Coordinated incident management –** That response to incidents isn't "sliced and diced" by administrative, operational, or jurisdictional boundaries.
- **Shared information –** That what is available or known to one is shared, as needed, with others.
- **Coordinated information management –** That the ever-present threat of "TMI" (too much information) doesn't cause the message to be lost among the noise.
- **Economies of scale –** That public funds are efficiently used for effective systems supporting all emergency response.

Evolving Communications Needs

Changes in how we manage resources and expect services to be delivered cooperatively have caused communications needs to evolve internally within organizations and externally between them. This has not occurred without great challenge.

For example, decentralized decision making and accountability—key principles in community policing—require that information be readily available to officers who are often widely dispersed throughout jurisdictions. Likewise, community oriented policing requires problem-solving partnerships between police, fire, EMS, and other public safety agencies. Those partnerships are strengthened when emergency service providers (police officers, firefighters, EMS, telecommunicators, emergency managers, etc.) have ready access to information from within their own organizations and elsewhere. Most often, that information is delivered to the field wirelessly.

One challenge that continues to plague emergency services is simply *how* to provide wireless coverage where they need it. It's an unfortunate, but inescapable, fact of today's public safety environment that the more widely dispersed responders are, the more difficult it is to provide them with reliable, high-quality voice and data network services. Officers in shopping malls, firefighters in large office buildings, and mountain rescuers alike are too often in unreliable margins of wireless communications and radio networks where information exchange is difficult. Relying on antiquated or obsolete equipment to connect responders can make coverage an even greater challenge.

Public safety agency managers have to work hard to assure that field personnel are reliably connected for safety purposes and for management of operations. While first responders are ideally always connected to the organizational infrastructure that supports their supply of and demand for information, the emergency environment doesn't always cooperate. Dense urban canyons, tunnels, ever-rising electronic noise, and system capacity issues are just a few examples of modern life that increasingly affect the wireless communications environment.

Communications interoperability is critical for information sharing.

Information powers the modern emergency services provider. Whether working individually or in tandem with others during a response, field personnel have to receive timely information about the incident, including location, scope, who else is responding, and tactical plans. Likewise, the information they provide in response can mean the difference between life and death for citizens, not the least of whom are the responders themselves.

Integration of information and communications systems—both between agencies and throughout field operations—is an essential part of interoperability today.

Developing Technologies

Figure 1-1: Detroit Police Department Station KOP (1928)

Radio communications is a key staple in the arsenal of public safety tools. It has only become more so in modern times.

Since the earliest systems built nearly 90 years ago, radio has been the primary means of getting information to the field. The Detroit Police Department had the first system licensed with the Federal Radio Commission in 1922, listed as KOP, an AM broadcast station required to transmit music between all-points bulletins and administrative messages, with no ability for field units to acknowledge receipt or reply to broadcasts (at times, that might still seem to be an advantage!). By 1928, the radio car was a key part of Detroit's policing environment.

How times have changed! While the melodious sounds of today's dispatches are hardly entertainment, our radio systems have come far from those one-way days. Gone is the time when radio simply served to connect responders and dispatch. Today, modern police, fire, and EMS agencies around the country rely on voice and data networks that share information wirelessly in all directions: vertically among levels of command, horizontally between functional subdivisions, and further yet across jurisdictional boundaries. Radios still connect responders and dispatch—but the *capabilities* of radio and the *training* needed to properly operate them have changed dramatically. Information is no longer shared only via "push-to-talk." Today's radios allow us to send text messages, make phone calls, and determine the real-time GPS location of the person carrying the device, among other uses. You can't hand a responder a radio anymore and train them by saying, "This is your life line. To use it, turn *this*, push *here*, talk *here*, and listen *here*."

Partners: Any agency, organization, or person that operates jointly or cooperates with your agency and with which you need to communicate.

Science and industry regularly improve our ability to make different technologies work together. Indeed, it's getting more difficult to distinguish radios from computers and wireless networks from wired pieces strung among them. Technological interoperability first achieved through integration of internal voice and data capabilities now allows us to connect similarly integrated systems with external partners.

This advancing technological environment makes it easier to share underlying parts of systems to take advantage of economies of scale, sharing what might otherwise be wasted capacity. Shared coverage and services are possible where completely separate systems were cost-prohibitive. Even though voice and data networks may be separate as they reach into the patrol car, many of the components up to that "last mile" can now be shared between agencies and systems. Both voice and data communications can pass over the same backbone network from dispatch to the transmission site. There they may share power, environmental, and antenna combining subsystems before parting company on separate frequencies destined for different radios in the car.

Elsewhere, developing technology has given us the means to get more users on a frequency, more data through channels, and the ability to assign "talk groups" dynamically based on the needs of the moment. Technology has evolved so that we can now link disparate radio systems, allowing users on one type of network to talk with those on another across their shared operational areas. And it has given us the ability to leverage the capabilities of wireless data to reduce demand for critical voice channels.

A technology environment that has made interoperability possible is just the beginning. We now need to determine how to work with the *increased functionality* but *remaining limitations* of these systems on a daily and/or emergency basis. This requires us to establish governance structures, develop policy, and provide ongoing training. Networking and connecting disparate groups is no longer just a technology challenge—it is also a *personnel* challenge. Agency personnel must develop relationships with other emergency service disciplines and develop policies for conducting interoperability activities so they are performed seamlessly when the need arises.

There's no doubt that technology advancements have dramatically changed public safety communications, particularly in the past 30 years. They have also challenged us to adapt business practices along the way, sometimes successfully, sometimes not. The growing array of choices we have will further challenge us to manage technology, rather than have it manage us.

The Interoperability Equation

In response to dramatic failures in interagency communications, government entities from Main Street to Pennsylvania Avenue have taken up the challenge of improving the situation. The term "communications interoperability" has come to mean different things to different people, especially following well-publicized breakdowns.

In order to bring focus to the subject, the national SAFECOM Program[1] was initiated. Communications interoperability is defined by SAFECOM as:

> *The ability of public safety agencies to talk across disciplines and jurisdictions via radio communications systems, exchanging voice and/or data with one another on demand, in real time, when needed, and as authorized.*

SAFECOM

An electronic government initiative housed within the U.S. Department of Homeland Security (DHS) designated as the umbrella program to coordinate Federal Government efforts to improve communications interoperability.

This ability to talk is the sum total of interagency operational plans, common procedures, and enabling technologies, multiplied by the effects of training and exercises. The best interagency plans and procedures are a complex function of standardized incident management systems and common terminologies. Funding and other resource limitations are often confounding factors in efforts to solve this equation.

Federal and state efforts have helped with this bit of algebra. The U.S. Department of Justice, through its Office of Community Oriented Policing Services (COPS Office), the U.S. Department of Homeland Security (DHS), through its Federal Emergency Management Agency (FEMA) and Office of Emergency Communications, and the U.S. Department of Commerce, through its National Telecommunications and Information Administration (NTIA), have cooperatively granted hundreds of millions of dollars to local agencies since the terrorist attacks of September 11, 2001, to improve communications interoperability. In addition, DHS has distributed billions of dollars to public safety agencies through State Homeland Security and Urban Area Security Initiative (UASI) grants, much going to improve communications in response to terrorist events. Funds provided through pre-existing federal grant programs in large share have been used to update and enhance the country's public safety communications infrastructure.[2] Unfortunately, economic downturns can significantly reduce the amount of funding available.

1. See www.safecomprogram.gov.
2. See www.grants.gov for information on federal grant opportunities.

In response, agencies at all levels may seek ways to get the most they can with the grant dollars they have remaining and leverage opportunities to co-locate, share services, or consolidate in some other manner.

Consolidating communications services or services level is not a new concept. However, a trend has emerged in recent years to support consolidation of some sort. Different variations of consolidation exist that provide different service levels and ultimately different outcomes. It could be a physical consolidation of Public Safety Answering Points (PSAP), consolidation of just the dispatch service, or becoming a "metro" or "public safety" agency. Consolidation can also mean sharing resources such as a radio system, computer aided dispatch, or information sharing systems. Each variation presents challenges and solutions along with other considerations that can leverage opportunities to improve interoperability. The question when it comes to consolidation for interoperability is, "Are we going to be able to communicate critical information better than we did before?"

At the state level, statewide interoperability executive committees—generically known as SIECs—have evolved to focus state and local efforts. First defined by the Federal Communications Commission (FCC) in 2001 for the administration of interoperability channels in the 700 MHz frequency band, SIECs have become pivotal in steering grant funds and growing multijurisdictional efforts in many states. Efforts in Washington[3] and Virginia,[4] for example, have provided models for how first responders across disciplines and jurisdictions can work together toward common goals. State homeland security agencies look to SIECs to connect their strategic plans with real-world interagency communications needs. The foundation for making these connections started through the development of Statewide Interoperable Communications Plans (SCIP).[5]

Besides the terror attacks of 9/11, Hurricane Katrina in 2005 was another landmark event that presented significant communications challenges. In response, on April 1, 2007, Congress created the Office of Emergency Communications (OEC) under DHS. Its purpose: "To promote the ability of emergency responders and government officials to maintain communication in the event of a natural disaster, act of terrorism, or other man-made disaster, and to ensure, accelerate, and attain interoperable and operable emergency communications nationwide."[6]

3. See Washington's SIEC website at http://siec.wa.gov/index.shtml.
4. See Virginia's interoperability website at www.vahs.virginia.gov/Initiatives/Interoperability.
5. See www.dhs.gov/files/programs/gc_1225902750156.shtm.
6. See www.dhs.gov/xabout/structure/gc_1189774174005.shtm.

In very short order, the OEC urged each state and territory to develop and submit a SCIP. These plans are living documents that should outline and define the current and future vision for communications interoperability within the state or territory. Creating a SCIP is no small task, so to help states and territories develop their SCIPs, the OEC provided technical assistance, outreach, and guidance. States that had implemented some form of a SIEC were better positioned than those that hadn't and were able to leverage that existing governance structure during this process. OEC support continues to this day through publications, guides, and annual SCIP Implementation Workshops. By April 2008, all 56 states and territories had established a SCIP.

To strengthen emergency communications capabilities during emergency events, an overarching strategy to help coordinate and guide interoperable emergency response was needed. Another act of coordination resulting from the OEC was the National Emergency Communications Plan (NECP), released by DHS in July 2009.[7] Adapted from SAFECOM's definition of interoperable communications, the NECP vision and desired future state is that:

> *Emergency responders can communicate as needed, on demand, and as authorized at all levels of government and across all disciplines.*

The NECP wasn't the first step toward improving interoperable communications. Rather, the NECP built upon successful work that had already taken place nationwide:

- Most federal programs that support emergency communications were consolidated within a single agency—DHS—to improve the alignment, integration, and coordination of the federal mission.
- All 56 states and U.S. territories developed SCIPs, Statewide Communication Interoperability Plans, that identify near- and long-term initiatives for improving communications interoperability.
- The nation's 75 largest urban and metropolitan areas maintain policies for interoperable communications.
- The SAFECOM Interoperability Continuum is widely accepted and used by the emergency response community to address critical elements for planning and implementing interoperability solutions. These elements include governance, standard operating procedures, technology, training and exercises, and usage of interoperable communications.

7. See www.dhs.gov/xlibrary/assets/national_emergency_communications_plan.pdf.

NECP Goals:

Goal 1: By 2010, 90 percent of all high-risk urban areas designated within the UASI are able to demonstrate response-level emergency communications within 1 hour for routine events involving multiple jurisdictions and agencies.

Goal 2: By 2011, 75 percent of non-UASI jurisdictions are able to demonstrate response-level emergency communications within 1 hour for routine events involving multiple jurisdictions and agencies.

Goal 3: By 2013, 75 percent of all jurisdictions are able to demonstrate response-level emergency communications within 3 hours, in the event of a significant incident as outlined in national planning scenarios.

- The DHS FEMA has established Regional Emergency Communications Coordination Working Groups (RECCWG) in each of the 10 FEMA regions to coordinate multistate efforts and measure progress on improving the survivability, sustainability, and interoperability of communications at the regional level.

Just like the SCIP development process encourages bottom-up development and stakeholder involvement, the vision and guidance for creating the NECP took the same approach. The NECP creation process included a lot of stakeholder input from all levels, especially the practitioner level. But there is no getting around it: The NECP is a complex document. The NECP establishes three goals, seven objectives, 29 initiatives, and 92 milestones. The content of the NECP is meant to provide guidance for achieving the three progressive goals by 2013. The clock started July 31, 2008.

With statewide interoperability governance taking hold and the benefits of coordination realized, states have further defined their interoperability efforts down to the regional level. A majority of states have identified a Statewide Interoperability Coordinator (SWIC). A significant majority of the states have come up with strategies to divide their state into regions. You can look to a state's SCIP for discussion on their regional boundaries.[8] States that have a UASI, meanwhile, were recommended by DHS to operationalize their SCIP by developing Tactical Interoperable Communications Plans (TICP). TICPs define what interoperability assets are available, how to request them, and the policies required to activate them. A handful of states have built upon that recommendation and have developed TICPs for each of their interoperability regions.

Efforts to solve the interoperability equation are probably affecting your work, whether you've been aware of it or not.

What Will Tomorrow Bring?

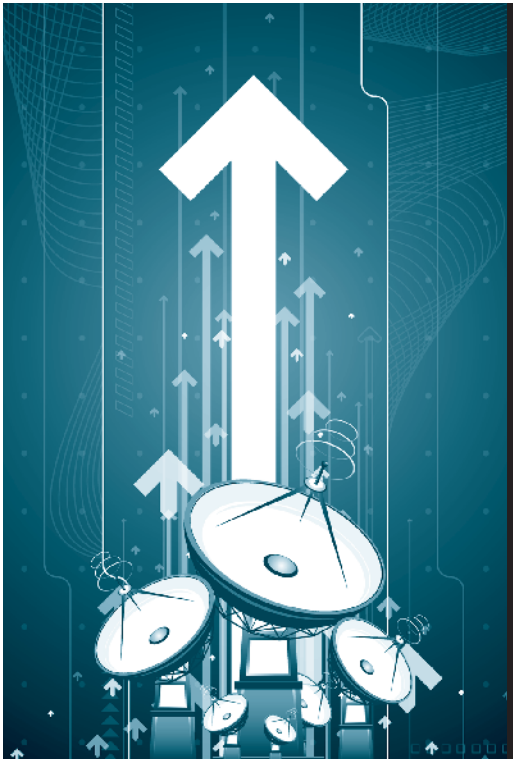
A coordinated effort to achieve interoperability continues to develop between federal, state, tribal, and local agencies. The NECP, statewide governance, and SCIP development dovetail to create a bottom-up approach to moving interoperability forward based on a common planning framework. This is a great start, but the work is far from over.

This is the environment faced by agency and project managers who are working to improve communications within their own jurisdictions. Perhaps you're reading this because you're responsible for making those improvements. How will it change over the period of your projects, the life cycles of your systems, or your career?

It's easy, if sad, to imagine that emergencies and disasters capturing national attention will continue to occur. Communications needs will evolve as our response capabilities become more complex and sophisticated. Technology will surely continue to offer opportunities for greater interagency communications and challenge our ability to employ it without disrupting what's already been achieved. And our collective efforts will help solve the interoperability equation.

In the chapters ahead, we'll look further at challenges to achieving interoperability—right after taking a brief look at how information flows in organizations with technology that is well integrated into services being delivered.

8. SCIPs are available by contacting the Statewide Interoperability Coordinator (SWIC) for the particular state.



CHAPTER 2

Key Challenges and Critical Elements

THE EVER-CHANGING ENVIRONMENT of public safety agencies has brought a range of challenges to achieving the communications interoperability necessary for emergency services. Nationally, the key challenges and critical elements for success have been documented through the collective attention of local, state, and federal officials. This high level of attention arose in concert with a growing public awareness of interoperability problems, and persists because interoperability problems are complex and not easy to fix. Though dramatically highlighted every time there is a tragic event, communications, particularly interagency communications, have long been a problem.

At the heart of public safety communications is field responder radio capabilities. Radio communications—or the lack thereof—can and has contributed directly to responder deaths. This Guide stresses that integration of voice and data technologies is necessary for interoperability, but we recognize from direct experience the importance of field responder voice communications. Radio is the most critical information technology tool for officers investigating a "hot" burglary, firefighters on interior attack during a structure fire, and paramedics providing advanced life support. Given its importance in basic emergency operations, there's no surprise that field responder radio capabilities are also at the heart of interoperability needs.

Why Public Safety Can't Talk

Following that fateful September day in 2001, the National Institute of Justice (NIJ), Office of Science and Technology, brought together the National Task Force on Interoperability (NTFI). The NTFI reported out five key reasons why public safety can't talk.[9] From policy and operations perspectives, they are:

- Incompatible and aging communications equipment
- Limited and fragmented funding
- Limited and fragmented planning
- Lack of coordination and cooperation
- Limited and fragmented radio spectrum

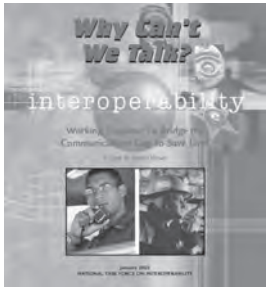


Figure 2-1: Why Can't We Talk? Working Together to Bridge the Communications Gap to Save Lives

9. *Why Can't We Talk? Working Together to Bridge the Communications Gap to Save Lives, National Task Force on Interoperability*, February 2003. Available at www.ncjrs.gov/pdffiles1/nij/204348.pdf.

Then, now, and into the future, every effort to improve interagency communications faces these same challenges, though to different degrees and for different reasons. For example, some jurisdictions have long histories of productive planning and coordination, but are desperately short of needed funds for system upgrades to connect responders across agencies. Other jurisdictions face such a severe shortage of radio frequencies that interoperability efforts are stymied, regardless of available funding. Each group of agencies seeking to improve interoperability faces a different combination of these basic challenges.

This eye-opening study was followed by a report that modernized views on what it takes to achieve interoperability—The National Interoperability Baseline Survey. The survey, which polled 22,400 agencies across the county, was conducted by SAFECOM in 2006 to measure interoperable communications on a nationwide level for the purpose of improving their effectiveness for emergency response practitioners. This study was different from work completed by the NTFI and others because it focused on five elements more commonly referred to as the *lanes* of the interoperability continuum: governance, standard operating procedures, technology, training and exercises, and usage. The outcome of the survey has helped agencies to do the following:[10]

- Determine the capacity for interoperable communications among law enforcement and fire response/EMS agencies across the nation
- Establish a process and mechanism to make it possible for agencies to regularly measure communications interoperability
- Help emergency response officials make better-informed decisions about how to most effectively allocate resources for improving communications interoperability
- Guide and measure the effectiveness of future communications interoperability improvement efforts that local, tribal, state, and federal emergency response organizations execute

The baseline survey provides a measureable starting point, a national forum to openly discuss the "reasons why" identified in the NTFI study, and a tool—the interoperability continuum self-assessment—to do something concrete about interoperability at their level.

10. www.safecomprogram.gov/baseline/Default.aspx.

There have been great successes at the state, local, federal, and tribal levels around the country and those successes should be used as best practice models. However, we should not lose sight of the fact that the lack of interoperability is still a real problem. The reality is that the issues identified by the NTFI still exist, and will continue to exist well into the future. Communications equipment continues to age, funding sources are more scarce, turf issues still exist, and limited spectrum issues will continue to grow along with the proliferation of mobile devices.

Other Interoperability Issues:

- 60,000+ public safety agencies with more than 2.5 million personnel
- Multiple disciplines (law enforcement, fire response, emergency medical services)
- Multiple tiers of government (township, city, county/parish, state)
- Technology differences (multiple system manufacturers, different communication modes, varied frequency bands)
- Operational differences between public safety disciplines
- Differences in rural versus urban mission operations

We'll get into how these challenges can be addressed in Part 2 of this Guide, **How is Interoperability Achieved?** But before we do, let's take a look at how these challenges have developed into persistent national problems.

Incompatible and Aging Communications Equipment

The life cycle for radio system infrastructure has traditionally been very long, sometimes exceeding 20 and even 30 years. Equipment used in these systems, such as your portable and mobile radios, has an expected 8–10 year service life, yet more than one-half currently exceed that age. The SAFECOM National Baseline Survey results indicated 25 percent of responding agencies reported their primary wireless systems were between 6–10 years old and 35 percent reported their systems exceeded 10 years.

60 percent of state and local law enforcement agencies report that aging radio communications equipment is a problem.

A survey of 1,334 state and local law enforcement agencies conducted in 1998 by the National Law Enforcement and Corrections Technology Center for NIJ showed a direct correlation between the age of systems and respondents' assessment of their radio communications effectiveness.[11] Sixty percent reported aging equipment to be a moderate to major problem. Local law enforcement systems averaged 9 years in service, while state systems averaged even longer—15 years. According to reports issued by Public Safety Wireless Network (PSWN), a joint initiative of the U.S. Departments of Justice and Treasury that is now part of SAFECOM, local fire and

11. Taylor, Mary J. et al., *State and Local Law Enforcement Wireless Communications and Interoperability: A Quantitative Analysis*, NCJ 168961, Washington, D.C.: U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, January 1998. Available at www.ncjrs.gov/pdffiles1/168961.pdf.

emergency medical services (EMS) systems average 10 years.[12] The results of the National Baseline Survey indicate higher levels of interoperability than expected, but there is no indication that the aging equipment statistics previously reported have improved to any significant degree since the 1998 report.

Options for police, fire, and EMS radios have flourished in recent history.

When characters Roy DeSoto and Johnny Gage showed us (well, at least some of us) just how exciting communications could be during the 1970s hit television show "Emergency!", radio technology choices were few and compatibility was high. Their call sign, KMG365, was and still is assigned to a VHF (Very High Frequency)-high band, analog FM (frequency modulated) base station. The call sign and station are still in use by Los Angeles County, although probably with equipment of more recent vintage!

Advances in technology may support sharing of resources, but a tight economy continues to hinder agencies from upgrading or replacing their aging systems. Unfortunately, some agencies are still using radios purchased new when "Emergency!" debuted. The simple fact that the radios still work is amazing. It says something about the quality of equipment manufactured for lengthy public safety use, but more about historically limited technology choices that lead (or force) agencies to upgrade. Options for emergency services radios have flourished, much the same way that we've seen wireless technologies explode in the consumer sector.

The costs of supporting old equipment, manufacturers dropping technologies, and mandates like narrowbanding, are leading agencies across the country to upgrade systems. Regional incompatibility grew rapidly as agencies upgraded one by one to meet pressing internal needs. Regional incompatibility may have slowed in recent years, but the problem persists because radio system life cycles vary, and separate agencies within a single jurisdiction end up needing to upgrade or replace systems at different times. The gap in capabilities between older and newer systems is getting wider and wider. Depending on the particular circumstances of the agencies involved, this could mean that waiting to make changes may result in more interoperability challenges rather than less. In many cases, partners and neighbors are simply unable to upgrade at the same time.

As a result of these challenges, we have, for example, rural fire departments using radio technologies pioneered more than half a century ago while larger, neighboring jurisdictions have migrated to higher frequency bands, digital channels, and trunked systems.

12. Public Safety Wireless Network Program Management Office, *PSWN Program Analysis of Fire and EMS Communications Interoperability*, prepared by Booz, Allen & Hamilton Inc., April 1999. Available at www.safecomprogram.gov/library/Lists/Library/Attachments/152/Fire_EMS_Interoperability_Study_Summary_Report.pdf.

Limited and Fragmented Funding

Across all levels of government, limited and fragmented funding has contributed to the interoperability challenges by:

- Hindering replacement of aging and incompatible equipment
- Restricting human resources available for interagency planning
- Forcing agencies to focus on their most pressing internal operational needs
- Limiting access to scarce radio spectrum resources

There are plenty of agencies that want to share and leverage resources to take advantage of improved technology and system capabilities. Paying a fair share of new system infrastructure or purchasing subscriber units to join an existing system where they are already in the coverage area still costs money that many agencies simply do not have. If an agency wants to participate but the reality is that they can't afford to do so, then the issue remains unresolved and incompatibility persists.

There has never been a national strategy for funding public safety radio costs. Local radio systems for police, fire, and EMS are funded by every means available to government, from general appropriations and bonds to grants and bake sales. Local, tribal, and state systems, alike, are most often funded as one-time projects. Their ongoing costs—including maintenance, licensing, network services, training, replacements, and other operating expenses—are annually shoehorned into tight budgets. By contrast, 9-1-1 services around the country are to a great extent funded similarly from state to state. Congressional action has helped standardize 9-1-1 funding and provide accountability for related expenditures.

The value of America's public safety radio infrastructure is staggering.

It's no wonder there is such fragmented funding for public safety radio. The value of America's investment in it continues to grow at a staggering rate. In 1998, the value of equipment and fixed infrastructure alone was estimated to be worth $18.3 billion.[13] This commonly cited figure does *not* include system installation, testing, training, or other implementation costs. Complete replacement of existing public safety radio systems, with all associated costs, would total two or more times this figure. The net effect of limited and fragmented funding for public safety radio systems is great diversity between systems and long replacement cycles across the country.

13. Public Safety Wireless Network, *LMR Replacement Cost Study Report*, prepared by Booz, Allen & Hamilton Inc., June 1998. This report and figure is currently the most comprehensive available for the replacement costs of land mobile radio (LMR) equipment owned by local, state, and federal government. Available at www.safecomprogram.gov/library/lists/library/DispForm.aspx?ID=96.

Limited and Fragmented Planning

Limited and fragmented planning is a key reason for interoperability problems. Agencies at all levels of government competing for limited funds have provided few resources for interagency planning efforts. This competition has compounded interoperability problems by discouraging partnerships necessary for joint operating plans that define communications needs.

Lack of Coordination and Cooperation

Radios on widely separated frequencies are incapable of being tuned from one to the other.

A lack of coordination and cooperation among agencies in funding and managing systems exists. Changing the pattern of isolated spending and increased sharing of management and control are necessary steps. While multiple solutions to meet varying needs are inevitable, portions of infrastructure, such as towers, and even full systems can be shared in some cases.

We'll have more to say about the importance of operational planning and coordination shortly.

Limited and Fragmented Radio Spectrum

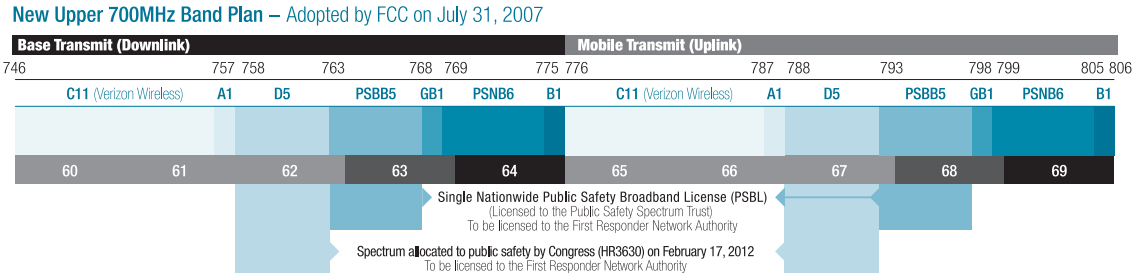
Agencies seeking to expand or upgrade their systems are increasingly being forced to move to higher frequency bands to find available channels. Because radio equipment is typically built to operate on a single one of the 10 bands open to public safety, systems using different bands are technologically incompatible at a fundamental level. That is, the radios talk on frequencies widely separated and are incapable of being tuned from one to the other.

More than half of all agencies operate in VHF-high band.

History and operational needs have crowded users to the lower ends of the spectrum. The vast majority of public safety radio systems—both voice and data—operate in four of the lower bands. More than half of the agencies in the country operate their primary voice systems in a single one: VHF-high band.[14] Additional channels in current bands are virtually unattainable in many parts of the country.

14. VHF-high band for local and state agencies runs from 150 to 174 Megahertz (MHz). According to supporting documents for PSWN's *LMR Replacement Cost Study*, nearly 57 percent of agencies make primary use of it, while fewer than 6 percent used 800 MHz. See study mentioned in note 13.

Figure 2-2: Public Safety Spectrum Allocation



When an agency moves its radio communications to a "new" band, the technological divide of operating across bands brings fresh challenges to talking directly with previous partners. Other technologies, such as console patches, have been used for years to link agencies on different bands. Newer multiband (multimode) radios that can operate in multiple parts of the spectrum are also an option. But these bring their own limitations and require additional planning. Remember the planning challenge? The most common approaches to resolving the effects of fragmented spectrum are, to put it simply, just patches. They're less than ideal, but unfortunately necessary.

Interoperability would certainly be an easier nut to crack if all agencies operated in the same range of radio spectrum. Unfortunately, each band offers a limited number of channels—the real estate of wireless communications. Each geographic region (neighborhood) only has a certain number of channels (residential lots).

"Location, location, location," they say in the world of real estate. Location in the wireless world is equally critical, but here we're not just talking about geography. We are also referring to where a system operates within the radio spectrum! Each of the 10 bands is best suited for different purposes and the highest ones are entirely unsuited for unit-to-unit voice systems as we know them today; they're used for microwave links. And needs vary across the country. For example, urban areas have great demand for channels in the higher bands offering the best building penetration. By contrast, wide-area systems necessary in rural and statewide jurisdictions are most economical in the lower bands where range is greatest. Remember the funding challenge?

The highest frequency bands are unsuited for voice systems as we know them today.

The net effect is best described as increasing fragmentation that reduces interoperability. Public safety has a growing need for wireless services beyond traditional voice operations. Mobile data, automatic vehicle location, and other types of systems increase demands on finite public safety spectrum. Beyond that, growing commercial and private demands for wireless services brings intense competition for limited resources that otherwise might be used for public safety. Rebanding, narrowbanding, and the D-Block are a few of the more contemporary approaches to alleviating spectrum problems, but these only scratch the surface.

Limited and fragmented radio spectrum is a fundamental cause of interoperability problems.

Critical Elements to Achieving Interoperability

Since 2003, the Department of Homeland Security SAFECOM Program has been working to bring a practitioner's focus to the problem of interoperability. Through SAFECOM, public safety leaders have identified five critical elements to solving interagency communications problems:

1. Governance
2. Standard Operating Procedures
3. Technology (Voice and Data)
4. Training and Exercises
5. Usage

They also identified stages along each element, recognizing that interoperability isn't an either/or proposition—it's a matter of degree. Interoperability improves as agencies progress with each of these elements. SAFECOM's *Interoperability Continuum*, found in this Guide as the foldout rear cover, depicts these elements and stages. These ideas are briefly summarized here and incorporated throughout this Guide.

Governance

Limited coordination and collaboration between agencies is a key reason why we can't talk. Regular collaboration between key staff members of agencies and across disciplines improves this situation, but formalized committees serving regional needs and working with statewide efforts are best. (For more information on Governance, see Chapter 5).

Standard Operating Procedures

All public safety agencies have established standard operating procedures (SOPs)—whether these are verbal or written. The level of interoperability between agencies increases as they create joint SOPs, typically first for planned events, then for emergencies. Interoperability improves as joint planning moves to serve regional needs, producing communications SOPs. Optimal levels are reached as the National Incident Management System (NIMS) is integrated into procedures. (For more information on SOPs, see Chapter 12).

The level of interoperability between agencies increases as they create joint SOPs, typically first for planned events, then for emergencies.

We'll talk further about the NIMS in Chapter 3, **Operability—Job #1**.

Technology (Voice and Data)

There are five identifiable technological means of interagency communications, particularly by radio:

1. Swapping radios
2. Using gateways between independent systems
3. Sharing channels
4. Sharing proprietary systems
5. Sharing standards-based systems

Higher levels of interoperability are reached as the predominant means progresses toward shared systems.

The National Incident Management System (NIMS)

[A] consistent nationwide approach for Federal, State, and local governments to work effectively and efficiently together to prepare for, respond to, and recover from domestic incidents, regardless of cause, size, or complexity.

—Homeland Security Presidential Directive (HSPD)-5
February 28, 2003

Technological Means to Interoperability
Swap radios
Use gateways
Share channels
Share proprietary systems
Share standards-based systems

A minimal level of interoperability is achieved when agencies resort to providing partners one of their radios, and vice versa, during incidents. This is what we refer to as "swapping radios." It's not ideal for a number of reasons, but has often been relied upon.

"Gateways" are electronic, often automated devices for taking the audio from one radio channel and patching it to another—and vice versa. In the past, the most common form of gateway was provided by the dispatch console patch mentioned on page 33. Since September 11, a great many of these have been purchased to improve interoperability. We'll delve further into these devices in Part 3 of this Guide, **Exploring the Technologies**.

A higher level of interoperability is provided when agencies using compatible technologies designate common channels between them for interagency communications in joint operations. This is referred to as "sharing channels."

The final two technological means of interoperability are more self-explanatory. Interoperability through "shared proprietary systems" occurs when multiple agencies jointly use a common system based on proprietary—or vendor-specific—technology. This is considered to be a less optimal means than shared use of a system built from standards-based—or non-vendor-specific—technology. Again, we'll go further into detail on these and other technologies in Part 3.

Training and Exercises

The importance of training and exercises cannot be overstated. Communications interoperability improves in small amounts through simple internal orientations on communications equipment. Tabletop exercises provide further improvements, but by necessity, these limit the number of people involved, typically to key field and support staff. Multiagency tabletop exercises produce a higher level of interoperability than single agency ones, of course. Full functional exercises between agencies involving all staff are optimally second only to regular, comprehensive training and exercises incorporating the regional SOPs described previously. (For more information on Training and Exercises, see Chapter 13).

Usage

Interoperability improves as agencies use their adopted techniques, procedures, and technologies more frequently and broadly. A minimal, but important, level is reached as those methods and means are used for planned multiagency events. It is further improved by common use during localized emergencies and further yet as incorporated into regional incident management systems. Optimal levels are reached as they are used on a daily basis throughout the region.

It's important to note that the steps from minimal to optimal levels of interoperability along each element in SAFECOM's *Interoperability Continuum* are progressive. That is, they build on one another and don't necessarily exclude preceding steps. For example, individual agency communications SOPs are still important when joint or regional ones are in place. Ideally, the two closely mesh. Likewise, in-service orientations on equipment are still important, even when regular, comprehensive regional training is in place.

One More Time: It's the Planning and Coordination

There's a lot more to be said about planning and coordination for interagency communications. As a matter of fact, that's what all of Part 2 is about! Well, it's mainly about how to achieve interoperability, but we'll give you a brief preview and let you know that's what it takes to get from here to there.

If it isn't already apparent, planning and coordination between agencies are the basic principles behind the Interoperability Continuum's critical elements.

No communications system can make up for inadequate operational plans.

Planning for interagency operations, generally, varies greatly from one part of the country to another as well as between levels of government. Where inadequate operational plans exist, communications suffer tremendously and interoperability is practically impossible. Poor communications can and unfortunately often do hinder operations, but no communications system or set of interoperable systems can make up for inadequate operational plans.

In Part 2 of this Guide, we'll show how communications interoperability is achieved through a common incident management system, technologies linking responders, and operational plans brought to life before they're needed through training and exercises.

The McKinsey Reports were prepared for New York City's police and fire departments in the year following the World Trade Center attacks on September 11, 2001. They include detailed analyses of response to the disaster and recommendations for improving preparedness in the future. We'll refer elsewhere to these reports on matters important to agencies of all sizes.

McKinsey Reports

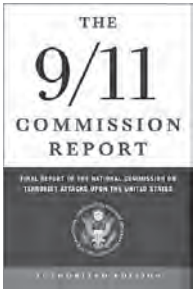
[T]o be fully prepared to face the threats posed by terrorism and other major incidents, the city or state governments must establish a much broader, detailed and more formalized inter-agency planning and coordination process. . . . The process would include:

- Establishment of common command and control structures and terminology, and agreement on the roles and responsibilities of each agency for managing the response to any incident.
- Deployment of interoperable communications infrastructures and protocols to improve response coordination and exchange of information.
- Implementation of joint training exercises to ensure that agencies can and will cooperate effectively during incidents, e.g., by operating under a unified command and control structure.

"Increasing FDNY's Preparedness," McKinsey & Company
August 19, 2002, Executive Summary, p 21.
Available at www.nyc.gov/html/fdny/html/mck_report/toc.shtml.

CHAPTER 3

Operability—Job #1



Command and Control within First Responder Agencies.

For a unified incident management system to succeed, each participant must have command and control of its own units and adequate internal communications.

The 9/11 Commission Report
(Page 319)

Throughout this Guide, we refer to the events of September 11, 2001, and after-action reports to highlight issues of interagency communications. The sheer magnitude of those events provides a powerful microscope for examining not only internal operational demands on agencies under such extraordinary circumstances, but also interoperability needs.

We all owe a huge debt of gratitude to the agencies rich with experience and history that hardly volunteered, but valiantly responded, that day and now share their lessons learned. We use those lessons here not critically, but to share the benefit of quality analyses arising from the World Trade Center and Pentagon maelstroms.

Though the magnitude of those events and scale of response are hopefully beyond what any jurisdiction will face in the future, our belief is that lessons highlighted here apply to public safety operations at all scales.

The level of attention brought to the national issue of communications interoperability has, at times drawn the spotlight from this fact: **Day in and day out, communication is critical in delivery of all sorts of public safety services.** As "operability" is the root of the word, it's also what makes interoperability possible.

The interoperability puzzle is solved by **first** resolving operational communications needs.

Interagency communications are, at best, a distraction if an agency is unable to provide for its own operations. At worst, they can bring chaos to emergency response if they interfere with internal operational demands. No agency administrator, chief officer, or incident commander wants to worry about how the troops are going to talk to other agencies when their own internal radio or other forms of communications are inadequate. The interoperability puzzle is solved by *first* resolving operational communications needs.

Before moving on to Part 2, which focuses on how interoperability is achieved, we want to emphasize the importance of beginning with an operational perspective. We'll look at some of the operational lessons learned during the 9/11 attacks and conclude with how standardized incident management systems provide tools to battle both operational and interoperability challenges.

A Proportional Perspective

In trying to understand what communications interoperability is and how it relates to daily requirements, it's important to note that radio voice communications is first and foremost the primary form of communication used for delivering services day-by-day to Mrs. Smith. Her emergency services are primarily provided by local agencies—usually by a single one for any given call. Consequently, the lion's share of public safety radio communications takes place internally between units of individual local agencies.

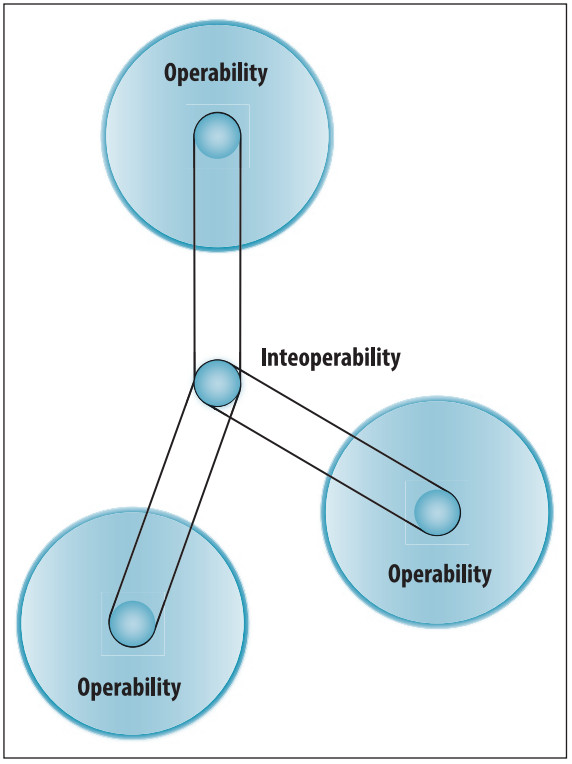
Operations, particularly the intersection of operational responsibilities between agencies, drives interoperability needs. That is, two agencies responsible for providing services at the same place and time need to work together to serve their missions. **However, internal agency communications demands overshadow interagency requirements even in large incidents because the bulk of traffic is still tactical within responding units, typically from the same agency.**

In terms of sheer volume, communications demands across all types of public safety response stack up like this:

1. Internal communications within individual local agencies
2. Interagency communications between like agencies from adjoining jurisdictions, such as between city police and county sheriff or between neighboring fire companies
3. Interagency communications between different types of responders, such as police and fire, in the same jurisdiction
4. Interagency communications between different types of responders in neighboring or distant jurisdictions

This isn't to say that any particular type of radio exchange is insignificant or expendable. It is important to note, however, that **day-to-day internal communications needs drive requirements for radio systems**. After all, there's no need to interoperate if you can't operate to begin with!

Figure 3-1: Operations Drive Interoperability Needs



While this might seem obvious, we've seen plenty of technology projects where basic needs are forgotten in the rush to find a "silver bullet" for a smaller set of problems. It simply boils down to the fact that internal operational needs are appropriately the central focus of agency radio projects. However, those needs can be defined, satisfied, and incorporated into standard operating procedures (SOPs) while assuring interoperability, as we'll see shortly.

Extreme Operations—9/11

A great deal has been written about emergency response in New York City during the World Trade Center attacks of September 11. In the year following the attacks, the New York City Police Department (NYPD) and Fire Department of New York (FDNY) collaborated with McKinsey & Company, business and organizational performance consultants, to produce reports on improving the agencies' preparedness. Though the reports contain much information on response during the incidents and detailed recommendations, we just want to touch on operational communications aspects they addressed.

At the time of the attacks, NYPD was operating with a new radio system that offered great capacity and resiliency over its previous systems. The police system also was significantly more modern than FDNY's, which had been struggling to implement a new one of its own.

According to McKinsey & Co., the police department's radio infrastructure did not fail on 9/11. Less than 15 percent of responding officers reported experiencing "dead air" failures. On the other hand, radio traffic was "cluttered" early in the incident. Fewer than half of the officers reported being able to clearly decipher traffic early on.

One of six critical recommendations made to NYPD focused on its radio communications. It recommended adoption of radio procedures that optimized information flow, producing a radio discipline that would minimize demand for channels and provide a capability to push critical information ahead of other traffic.[15]

FDNY communications were affected directly by the attacks themselves. Overall, their radio system was inadequate for the scale of the incident. McKinsey & Co. found that the department urgently needed to improve its communications capabilities and ability to pass along critical incident information. Information management improvements were also noted as urgently needed, particularly in tracking responders and patients.[16]

15. McKinsey & Company, *Improving NYPD Emergency Preparedness and Response,* August 19, 2002. Available at www.mckinsey.com/locations/madrid/pdfs/nypdemergency.pdf.

16. McKinsey & Company, *Increasing FDNY's Preparedness*, Executive Summary, August 19, 2002. Available at www.nyc.gov/html/fdny/html/mck_report/toc.shtml.

Important Conclusions

Two important conclusions can be drawn from these findings:

Conclusion #1: An agency's internal operational *capacity* to receive, digest, disseminate, and act on information can be overwhelmed, even if technically its communications systems aren't. Operability is directly affected by nontechnical pieces of response systems that define, among other things, rules for moving information around and what constitutes a manageable span of control. Technology can deliver information overload as well as it can solve problems.

Conclusion #2: The great bulk of information sharing needs between first responders—and thus communications capacity of one form or another—are internal.

Judging from these reports, communications operability was a greater problem in New York City on 9/11 than interoperability. We believe this would be true in most any jurisdiction under comparably taxing circumstances, mainly because the agencies' own management needs become critical as they struggle to maintain a manageable span of control and accountability of responders.

National Incident Management System

Thankfully, national disasters of this magnitude are rare. Terrorist attacks and weapons of mass destruction have captured the nation's attention, but natural disasters and large-scale emergencies like wildland fires and hazardous materials incidents are more likely to happen across the country. Communications operability and interoperability needs have to be accommodated to support response to all scales of emergencies.

Procedures for day-to-day interagency operations are usually well-established.

Incident response systems have been built to meet the daily public safety demands, as well as the more predictable emergencies. Incident management systems vary widely across the country, but procedures for day-to-day interagency operations are usually well established because they're used relatively often.

Similarly, planned events and task force operations, such as political conventions or joint drug interdiction efforts, give incident command teams the opportunity to build solid plans beforehand. This includes plans necessary for interagency communications.

But when large-scale emergencies and disasters occur, response and communications systems are stressed. Informal incident management systems dissolve.

The National Incident Management System (NIMS) was introduced in March 2004. It is first and foremost a common set of concepts, principles, terminology, and technology to improve emergency response. It also provides standard resource, organizational, and operational definitions. One of its components is an incident command system familiar to many responders across the country.

The NIMS Incident Command System (ICS) is built from 30 years of experience with large-scale emergencies. Based on military models, early incident command systems emerged in the public safety world through efforts of California firefighting and emergency management agencies to deal with devastating wildfires. It broadened and evolved over the years to serve emergencies and disasters of all types.

Two key ICS management characteristics are particularly notable when it comes to communications interoperability. NIMS ICS is based on:

1. **Common terminology** covering organizational structures, operational resources, and facilities
2. **Integrated communications**, including development and use of a common communications plan covering processes and technology[17]

Common Terminology

The importance of common terminology is clear in interagency communications since it's not much use to talk to your cooperating neighbors if you can't understand them! But the concept goes much further.

Interoperability is built upon common terminology.

As mentioned earlier, lack of planning and coordination is a prime cause of communications interoperability failures. Planning and coordination requires a common language to articulate needs, describe processes, establish policies, craft joint SOPs, and command resources during interagency operations. Interagency communications SOPs are particularly unlikely without a means of describing the "who, when, why, where, what, and how" of operations.

We deal with practical and important aspects of common terminology in Chapter 12, **Develop Policies and Procedures**.

17. U.S. Department of Homeland Security, National Incident Management System, December 2008. Available at www.fema.gov/pdf/emergency/nims/NIMS_core.pdf.

Integrated Communications

Under ICS, communications and incident action plans have to be integrated to capture management goals and operational objectives. This notion of integration is more than just lip service, too. Since responder safety and effectiveness are usually closely related to how well communications supports them, the capacity of the communications systems to support operations is continuously taken into account in action planning. A separate communications unit is often established early in multiagency and large-scale responses managed under ICS to support the integration effort. This is to bring all communications functions close to incident management, rather than having them managed far from pressing operational considerations.

> How we play at the occasional "big one" will be determined mostly by how we play at the frequent little ones that occur every day in our local place.
>
> — *Fire Command Chief Alan Brunacini, Phoenix (Arizona) Fire Department*

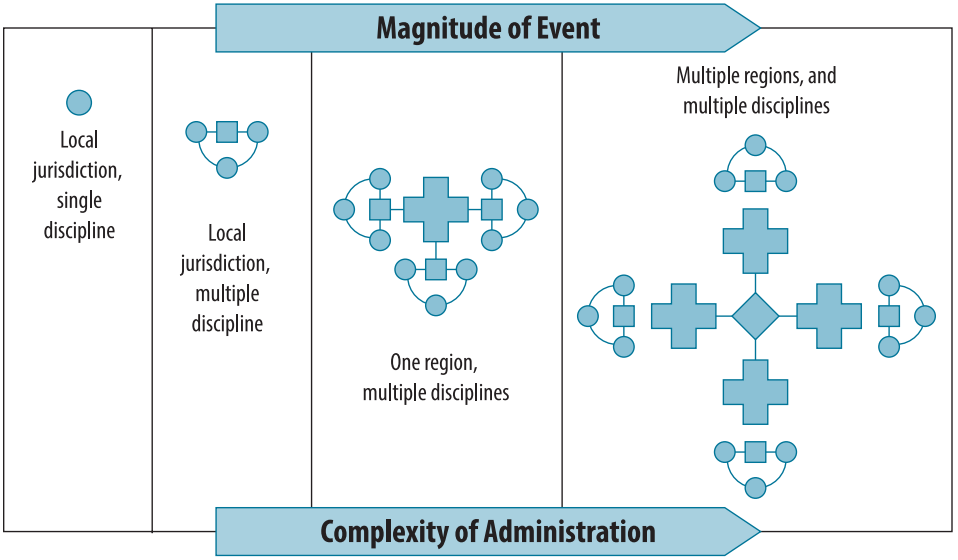
The incident communications unit is expected to quickly provide all aspects of communications. Particularly in the All-Hazards environment, you can't just *say*, "We have a communications unit." Communications resources are not magically going to start coordinating themselves. The unit needs staff. To help fulfill all the responsibilities, a fully staffed communications unit features a number of personnel in a variety of roles. Not every incident will use all the positions. However, the main position to fill is the Communications Unit Leader (COML). The COML is the key person to plan and manage the technical and operational aspects of the communications function during an incident or event.[18]

Traditionally, incident communications units are staffed with personnel from the road. The ranking officer enlists the closest firefighter or police officer and says, "Here, talk to dispatch." To manage the complexity of today's communications systems, personnel in these roles need training. You can't just improvise and expect everything to go perfectly. Standardized training is available nationwide for a variety of communications unit positions, including the Communications Unit Leader (COML) and Communications Technicians (COMT).[19] Communications plans and technology can be used to reinforce the command structures and operating principles embodied in incident management systems. To improve communications integration, public safety leaders should include communications unit personnel in incident training, planning, and response sooner rather than later. Each State is also encouraged to keep a current database of credentialed COMLs and other incident communications unit personnel.

18. For more information regarding the background of communications within the National Incident Management System and its Incident Command System, refer to COPS Issue Brief #2, *Communications in the Incident Command System*. It examines the role of communications within these constructs, as well as in the context of multiagency response to disasters and emergencies; it concludes with operational best practices for effective use of incident communications units. See http://ric-zai-inc.com/Publications/cops-w0422-pub.pdf.

19. See http://training.fema.gov and www.dhs.gov/files/programs/gc_1286984043354.shtm.

Figure 3-2: Interoperability Built on Separately Operable Systems



Source: U.S. Department of Homeland Security, SAFECOM Program.

The database should be accessible by State and local emergency management coordinators, SWICs, State Training Officers, police and fire chiefs and others that may be called upon as an Incident Commander.

Use of a NIMS-compliant incident command system is critical in a large-scale response. It can be equally important during smaller emergencies that provide the opportunity to perfect a response. Common terminologies and principles of communications integration take root in routine response. They provide the building blocks of interoperability through better operability.

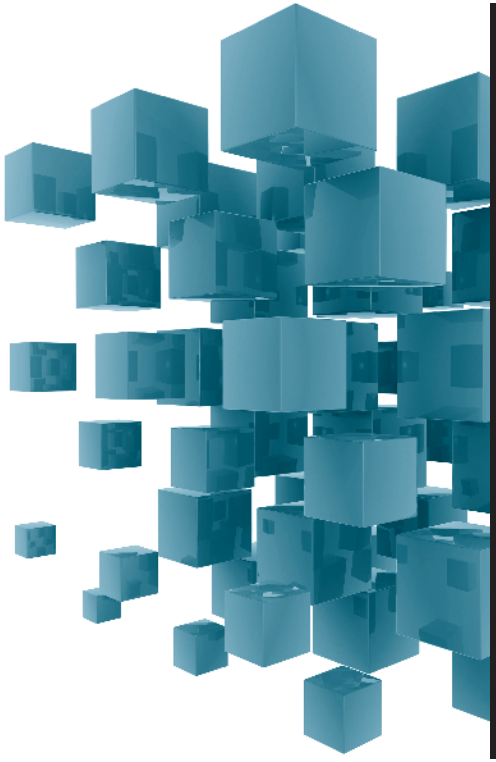
Operational Building Blocks

Interoperability is built up from separately operable systems. It's a defining quality of a system of systems. For example, the modularity and scalability of modern incident command systems mean they are useful from small incidents to large-scale emergencies. Separate command teams can even be folded into one as incidents merge. Components can be mixed and matched as demands ebb and flow.

Communications systems meant to serve such command systems have to be equally modular and scalable. Those capable of supporting an agency's operations have to be built to "plug and play" during multiagency responses, so it pays to build them with NIMS principles in mind. It also pays to keep continuity of operations in mind. Planning for the continuity of operations for the physical and human resource-related pieces of your communications systems are vital functions. They should be addressed as part of your continuity of operations planning (COOP) activities.[20]

While operations come first, interoperations are inevitable. Building command and communications systems for interoperability across jurisdictions and disciplines is just good business.

20. See www.fema.gov/about/org/ncp/coop/index.shtm.



CHAPTER 4

Interoperability in the Integrated Enterprise

PUBLIC SAFETY SERVICES ARE PROVIDED across all levels of government, through local, tribal, state, and federal agencies. The vast majority of existing communications infrastructure for delivery of these systems, however, is owned by local and state agencies—an ownership level estimated at more than 90 percent.[21] Cities, towns, and counties use their systems to provide essential police, fire, and EMS services at all hours of the day, every day of the year. For the most part, it seems that public satisfaction with these services is good, but there is certainly the expectation that agencies can work together when needed—in effect, that they're *interoperable*.

Readers may be interested in Chicago's enterprise criminal justice information system. See *Policing Smarter Through IT: Lessons in Enterprise Implementation*, Northwestern University, U.S. Department of Justice, Office of Community Oriented Policing Services, 2004.

See http://ric-zai-inc.com/Publications/cops-p059-pub.pdf.

To understand the demand for interoperability, we have to look at a picture of emergency services greater than individual agencies and their separate responsibilities. In wrapping up our discussion of just what communications interoperability is, we want to describe the public safety enterprise, its complexity across systems, and what integrating it entails. We'll look at why information sharing is at the heart of communications interoperability, how justice integration efforts laid a foundation for understanding needs, and the importance of stating functional and operational requirements to integrate systems. Your contribution to achieving interoperability is our central focus, so we'll conclude by looking at the role of leadership in the integrated enterprise.

What is the "Enterprise"?

The term "enterprise" is more and more commonly used to describe government and individual agencies organized to deliver particular services. For example, we speak of police, prosecution, courts, and corrections across local, tribal, state, and federal levels of government as the *justice enterprise*. Recognizing that each level of government and most of its branches are defined in law, it still has been useful to look at justice agencies as a single entity dealing with a related set of services for a common constituency. Integration of services and technologies across the justice enterprise allows each agency to better serve its customers, while minimizing costly redundancies and technological roadblocks.

An enterprise is a collection of agencies or organizations created to provide related services to a common set of customers.

21. U.S. Government Accountability Office, *Homeland Security: Federal Leadership and Intergovernmental Cooperation Required to Achieve First Responder Interoperable Communications*, GAO-04-740, Washington, D.C.: July 2004, p. 8.

FACTS:

- Interoperability is achieved when services are delivered seamlessly across organizational subdivisions and between jurisdictions.
- An enterprise view of public safety services—for example, across a city, county, or metropolitan region—uses a citizen-centered, results-focused definition of services provided to define, among other things, necessary interagency information exchanges.
- With services and these interagency junction points defined, a technological framework can be built that leverages existing investments and capabilities, reduces redundancies, and establishes de facto standards for future systems.
- Both services and supporting systems have to be integrated for the public safety enterprise to have communications interoperability.

All the policies, procedures, skills, and technologies that go into delivering effective emergency response need to come together at that moment, at that spot.

A Complex System of Systems

Modern agencies have a staggering array of complex systems supporting their services. How complex? Consider a typical call that's handled thousands of times each day across the country: a landline telephone call reporting a motor vehicle accident with injuries.

The Call Arrives

From the 9-1-1 call, an automatic call distributor may first direct the connection to an open attendant position, providing automatic number identification (ANI) information from the call. In the background, call-logging recorders track the source, routing, and conversations. An instant playback recorder may begin to capture the conversation for the operator's subsequent use while an audio logging recorder elsewhere makes a more permanent record. Where enhanced 9-1-1 (E9-1-1) is available, the caller's location is automatically identified (ALI) based on the master street address guide (MSAG), retrieved, and provided to the call-taker. The call to the public safety answering point (PSAP) is then either dispatched by the call-taker or transferred to a dispatcher across the room or perhaps even across town.

These acronyms and others are defined in Appendix F.

And that's all before response is initiated. E9-1-1, ANI, ALI, PSAP, MSAG....There's certainly no shortage of acronyms in the public safety communications business! But wait, there's more.

The Call is Dispatched

If the call-taker hasn't already done so, the incident might automatically be queued to a computer aided dispatch (CAD) system at this point—or maybe even separate CAD systems for fire medical and police response. The CAD system itself is a complex animal. From this point, it may interface through a general purpose console with telephone, alarm, paging, voice radio, mobile data, and logging systems. It might be fed mapping information in the background for geographic display of call source, caller location, responder location, and street closure indications. For later use, it might feed incident information to an agency's records management system (RMS) or simply drive a run card printer in a distant fire station.

Field Responders Respond

From dispatch, let's imagine that fire medical responders are alerted by a page and police officers by a message sent wirelessly to the squad car's mobile data computer. By way of a couple of key presses, the police officer acknowledges receipt of the alert and notifies dispatch of an impending response with lights and siren. Paramedics grab the run card, jump in their vehicle, and transmit acknowledgment of the call over a voice radio system. En route, automatic vehicle location (AVL) systems in each unit may transmit current location information to dispatch from a global positioning system (GPS) receiver for display on a geographic information system (GIS)-powered map in dispatch. On scene, the officer quickly transmits an arrival status message and turns to a shared radio channel to direct paramedics in from an alternate direction because the roadway is blocked by backed-up traffic.

Service is Delivered

Response is well underway, with a great deal of technology enabling it. A transporting ambulance may have been dispatched by this point and street maintenance alerted to divert traffic around the accident. Medical control may have been established through a nearby hospital and its emergency room notified of the impending arrival of patients. More systems are tied in. Eventually patients are delivered, cars towed, accident and run reports filed, and responders returned to routine duties.

This complex system of emergency services is linked through an integrated mesh of communications and information systems.

The hapless victims of our hypothetical accident don't know—and probably don't care at the time—about all that goes into delivering emergency services to them. All they know is that they need help. All the policies, procedures, skills, and technologies that are involved in delivering effective emergency response need to come together at that moment, *and* at that spot.

Enterprise Integration

This example provides a snapshot of the public safety enterprise. It shows the complexity of technologies used to support emergency operations, generally, and interagency operations in particular. Information flowing across wired and wireless networks, through computers and voice systems, allows interagency services to be delivered seamlessly. It allows them to be *integrated* across the public safety enterprise.

When communications break down, who are you going to call? 9-1-1?

Information is moved from place to place through different systems and modes of sharing. For example, the location of this hypothetical incident most likely would have initially been reported by voice over the telephone. Nearly simultaneously, the call-taker received a street address or at least an idea of the general vicinity of the accident from the caller's location information retrieved digitally with the call. That location was displayed textually and later, perhaps, also graphically for the dispatcher. More and more commonly these days, a precise location may have been automatically transmitted wirelessly via satellite by one of the involved vehicles, and then relayed via telephone to dispatch by a telematics operator, such as OnStar®. In our example, the incident location was subsequently passed wirelessly to the field using both voice and data.

Perhaps you have already faced the challenge of integrating systems to deliver information so complexly. If so, you're one step up on the broader challenge of providing communications interoperability. You understand that a lot more than technology goes into making systems talk to one another. And if you've been responsible for connecting services across agencies, you probably already recognize that no amount of interoperable technology will bring responders together when their operations are fragmented. All the king's horses and all the king's men can't make one response out of many if *procedurally* agencies aren't "inter-operational" already. This, quite frankly, has nothing to do with technology.

How Did Communicating Get so Complicated?

Historically, communications interoperability has *diminished* as technology has advanced. This might seem counter-intuitive, but think about it. When there were few choices for communications technology, the odds of any two agencies having compatible technology were relatively high. Advancing technology, which brought more communications choices, has come up against long radio system life cycles and widely varying needs. Agencies have built advanced radio systems to solve serious coverage and capacity needs, inadvertently introducing new interoperability challenges. In effect, our technological options have expanded, spotlighting the "dis-integrated" enterprise that previously had been able to hang together due to fewer demands and greater technological homogeneity.

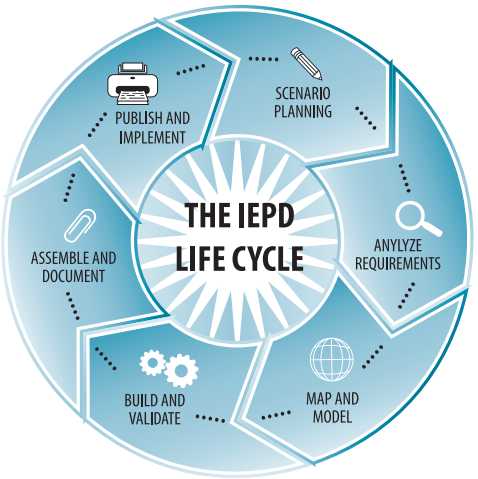
As noted earlier, aging and incompatible equipment is just one of several challenges to achieving interoperability. Suffice it here to say that a lot more than technology is needed for success.

The regular occurrence of events and disasters has highlighted greater needs for sharing information and coordinating incident management across all emergency services. Effective information sharing means information is available when needed, to those who need it, and who are authorized to have it. This requires communications interoperability. Ultimately, an enterprise view of services integrated across procedures and technology is necessary to satisfy these needs.

A Vision of Information Sharing

Information sharing is a measurable outcome of communications interoperability. On a daily basis, critical information most often passes between field responders by voice over radio. It can also originate from CAD, RMS, GIS, disaster management, state motor vehicle, and other systems, including e-mail, telephone, or even paper. From these systems, the information may be transferred to the responder wirelessly, to a mobile computer system, or it may make the leap from mere data to true information through the time-proven radioed voice of dispatch.

Figure 4-1: NIEM IEPD Life Cycle



NIEM includes a six-step life cycle that enables information exchange interoperability

In the public sector, some of the greatest advancements in information sharing have occurred through the U.S. Department of Justice's Office of Justice Programs and its Global Justice Information Sharing Initiative—generally referred to simply as "Global." The Global Advisory Committee (GAC) has served as an advisory body to the U.S. Attorney General since 1998. Its mission is to support broad exchange of justice information across jurisdictions and levels of government. It "seeks to improve the administration of justice and protect the nation's public by promoting practices and technologies for the secure sharing of justice information."[22]

Since September 11, Global's scope of advice has expanded to the broader public safety enterprise. For example, the Global Justice XML Data Model (GJXDM)[23] and its successor, the National Information Exchange Model (NIEM),[24] have significantly impacted the design of CAD and RMS for information sharing. Information sharing concepts have evolved greatly through efforts to integrate justice systems.

A domain is a business enterprise that is organized or affiliated to meet common objectives and is actively leveraging NIEM. The number is growing but 12 domains currently participate in NIEM across federal, state, local, tribal, industry, and international levels. Besides justice, some examples of domains are immigration, emergency management, and maritime.

Two other Global initiatives of national importance are the NIEM and the Global Reference Architecture (GRA)—we'll introduce NIEM here and talk about GRA a little further on.

NIEM is a national effort—sponsored by the Federal Government but with involvement from state, local, tribal, and international government representatives—to provide a common vocabulary and set of tools that support information exchange among justice, public safety, homeland security, intelligence, health, and many other domains. NIEM addresses the problem of individual agencies or jurisdictions using different terminology to describe the same thing, which has traditionally obstructed effective information exchange. NIEM allows these independent exchange partners to maintain control over their internal business processes (including terminology), while agreeing more easily on the terminology to use when they *exchange* information among

22. Global Justice Information Sharing Initiative Advisory Committee Charter, October 15, 2002.
23. For further information on the Global Justice XML Data Model, see http://it.ojp.gov/jxdm/.
24. For more information on NIEM, see www.niem.gov.

themselves. While the NIEM data model and tools provide the building blocks of virtually any information exchange, it is often easier for NIEM users to leverage the work of others. Chances are that someone, somewhere has already built a definition of an exchange that other jurisdictions or agencies can reuse (tweaking as necessary). In fact, there is even a repository of reusable exchange definitions (called Information Exchange Package Documentation (IEPD)) that contains hundreds of models, including models of CAD–RMS, CAD–CAD, and RMS–RMS exchanges.[25]

Global has provided a vision of information sharing that is very applicable to communications interoperability.

Vision Statement

Emergency responders can access the information they need to do their jobs, at the time they need it, in a form that is useful, regardless of its location.[26]

Such a vision would be followed by more specific goals laying out how the project will improve procedures and systems to ensure that the needed information is shared. The Global Infrastructure/Standards Working Group has established requirements for justice information sharing[27] that are equally applicable to interoperable communications systems:

- The architecture must recognize innumerable independent agencies and funding bodies from local, state, tribal, and federal governments.
- Information sharing must occur across agencies that represent divergent disciplines, branches of government, and operating assumptions.
- The infrastructure must be able to accommodate an infinite range of scales, from small operations with few participants in a rural county to national processes that reach across local, state, tribal, federal, and even international boundaries.

25. See the IEPD Clearinghouse at http://it.ojp.gov/default.aspx?area=implementationAssistance&page=1108.

26. Adapted from *A Framework for Justice Information Sharing: Service-Oriented Architecture* (SOA), Global Infrastructure/Standards Working Group, December 9, 2004. Available at http://it.ojp.gov/documents/20041209_SOA_Report.pdf.

27. Ibid., pp. 2–7.

- Information sharing must occur among data sources that differ widely in software, hardware, structure, and design.
- Public sector technology investment must reflect and incorporate the lessons and developments of the private sector.
- The infrastructure design must be dynamic, capable of evolving as the information sharing requirements change and the technology is transformed.

These are worthy strategic goals for all communications interoperability projects.

Information Sharing Concepts: SOA What?

For such a simple term, "information sharing" can be a complex subject. Some of the concepts and terms are simply too important to ignore, though. Notions of communications interoperability are being influenced by lessons learned through justice integration efforts, and familiarity with these ideas will help you understand the "big picture."

For example, work conducted by SEARCH in the field of justice information exchange modeling has produced a conceptual framework for understanding the flow of information between agencies, a methodology for analyzing and reengineering processes, and tools for modeling information exchanges. This work has expanded into characterizing, classifying, and quantifying first responder interagency communications.[28]

One goal of the modeling methodology is to produce a reference model—a set of exchanges common across most jurisdictions. This has been done for integrated justice information systems, resulting in a significant savings in effort and cost for subsequent users. Such a model can be customized by individual jurisdictions to reflect their operations, as-is, and portray their systems to-be, requiring a fraction of the effort needed to create one from scratch.

28. SEARCH undertook two projects to develop information exchange package documentation for tribal, law enforcement, and other first responders. These projects were funded by the COPS Office under Cooperative Agreements #2002-CK-WX-K006 and #2002-CK-WX-K047. For a description, see Law Enforcement Exchange Package Documentation, http://search.org/programs/info/publications/.

Common Terminology Aids Communication

Shared concepts and terminology have advanced the abilities of researchers and practitioners, alike, to describe dimensions and modes of information exchange.[29] In addressing functional components of integration, we now talk about query, push, pull, publish, and subscription/notification modes of communications. In integrated systems, **queries** make a specific request for information. Information is **pushed** automatically to other systems following triggering events. Likewise, it may be automatically **pulled** from others in anticipation of need. Information is **published** for general authorized consumption as a proactive measure. A **subscription/notification** process combines push and pull modes of information sharing on a more ad hoc basis controlled by the eventual user.

The importance of these terms and concepts is not so much that they bring some great revelation of how we might share information, but rather in providing a common terminology useful for stating requirements in a standardized manner through which a system of systems can be designed. For example, we may require that stolen vehicle information is pushed to an officer whenever a traffic stop is made. That tells a business process analyst or system designer that certain exchanges are required without further, overt action by the officer. However the information is ultimately provided—whether it is wrapped in standard operating procedures by voice from dispatch or encoded in the rules of a mobile data system—is a subsequent matter of design, and is probably influenced by additional requirements.

A final concept of growing importance in justice integration, as well as the larger world of automation, is *service-oriented architecture* (SOA). SOA views information exchange simply as a collection of services that communicate with one another using standard (non-proprietary) protocols. These services are designed, first and foremost, with reusability and flexibility in mind, so that future information exchange applications can build upon work done in the past. For example, Wisconsin uses a SOA-based message switch to move information from different sources to and between law enforcement agencies across the state.[30]

Service-oriented architecture (SOA) is a collection of services that communicate with one another.

29. David J. Roberts, *Integration in the Context of Justice Information Systems: A Common Understanding*, Sacramento, California: SEARCH, The National Consortium for Justice Information and Statistics, updated 2004. Available at www.search.org/files/pdf/Integration.pdf.

30. See www.doj.state.wi.us/les/TIME/eTIME.htm.

SOA means a great deal more in the design of integrated systems than is addressed here, but its influence on developing enterprise information systems is important. Public safety information and communications systems—as well as broader government systems—are increasingly being built upon SOA. The integrated enterprise also increasingly relies on this architectural framework.

Now that we've introduced SOA, let's circle back and talk a little more about the Global Reference Architecture (GRA) initiative. In 2004, Global recommended the justice community adopt SOA as a standard approach to justice and public safety information sharing.[31] However, the Global leadership also recognized that implementing SOA properly and with minimal cost would present a significant challenge to many justice and public safety partnerships across the nation. Accordingly, the Global Infrastructure/Standards Working Group began work on a *reference architecture* for SOA, called the GRA, and completed an initial version of the architecture in 2009. The GRA is primarily intended to provide the bulk of what agencies and jurisdictions need to implement SOA in their environment, from technical specifications to setting up proper governance to acquiring the right technology infrastructure. It contains methodologies and tools that allow information technology architects and analysts to capture business problems and define the right solution services quickly. It also shows how to use the sometimes bewildering array of national justice community standards—such as NIEM, the Global Federated Identity and Privilege Management (GFIPM) guidance, and the Logical Entity Exchange Specification (LEXS)—together effectively to support information sharing.[32]

The following are accepted guiding principles of integrated justice information systems, which influence our conception of what's possible with communications interoperability:

- Information exchange modeling
- Functional components of integration
- Service-oriented architecture

They can help us understand information sharing needs across a complex enterprise to achieve interoperability.

31. *A Framework for Justice Information Sharing: Service-Oriented Architecture (SOA),* http://it.ojp.gov/default.aspx?area=globalJustice &page=1235.

32. For more on the GRA, see http://it.ojp.gov/default.aspx?area=nationalInitiatives&page=1015.

Stating Requirements for Information Sharing

Our success in creating communications interoperability is directly related to our ability to describe operational requirements for interagency exchange of information. Projects to improve interoperability may be well-guided from the start with a broad *vision statement*, such as that presented above, but they have to develop *operational and functional requirements* in order to yield communications systems that meet day-to-day needs. Unfortunately, system procurement documents often focus on technical requirements rather than operational needs. This limits proposed solutions and forces acceptance merely based on technological measures.

When information sharing works, it is a powerful tool.
— The 9/11 Commission Report *(Page 419)*

In seeking to improve interoperability, we talk about police department 'A' needing to talk to fire department 'B' or something similarly broad. Left with no better description of the processes, events, conditions, and content of the needed communications, system designers get a one-dimensional picture of what's needed. Interoperable systems design is driven much more by operational requirements when, for example, the need is described as:

> *During a barricaded suspect operation, the police tactical team leader* **notifies** *the fire interior attack crew leader that suppression efforts are needed within a secured portion of the building.*

It may seem obvious that the need would be satisfied by a common radio channel or talk group readily available for a voice exchange between portable radios. That may be the most common way to carry the exchange today, but it may be equally well accomplished by status and location data burst across a network established just for the incident. Over-specification of how needs are met ends up limiting options and is often used as a substitute for a clear statement of business practices. The point is that the "how" should come long after operational and functional requirements are established.

Our success in creating communications interoperability is directly related to our ability to describe the operational requirements for interagency exchange of information.

It may also seem that describing interagency communications needs in such detail could be painfully tedious. Frankly, it can be. Unfortunately, the likely alternative is acquiring systems that are designed based on gross and largely unshared assumptions of the "who, what, when, why, and how often" aspects of interoperability. If procedures don't exist to describe how police operations communicate a need for help when a diversionary device ignites a fire, then the presence of the technological *capability* to talk is unlikely to be used effectively.

Broad statements of need that lack functional and operational requirements often result in technology project failures.

Efforts in information exchange modeling have shown that voice communications are not as neatly describable as data exchanges. But because voice and data are so intimately intertwined in the integrated enterprise, we're called to do our best in describing all types of exchanges so the boundaries between different modes of communications are clear. As importantly, voice exchanges may prompt subsequent data exchanges under certain conditions and vice versa. It's important to recognize these interactions—at least in operational procedures, if not also in technology.

The Good News on Stating Requirements

A good deal of work in recent years has been done to both define information sharing requirements broadly, and to improve our understanding of them.

Despite the problems that technology creates, Americans' love affair with it leads them to also regard it as the solution. But technology produces its best results when an organization has the doctrine, structure, and incentives to exploit it.

The 9/11 Commission Report (Page 88)

In March 2004, SAFECOM released a report establishing current and future requirements for public safety wireless communications and interoperability. This "Statement of Requirements" (SoR) established operational requirements for police, fire, and EMS services, as well as their wireless communications functional requirements. Now a two-volume set as of 2008, the SoR is currently known as the Public Safety Statement of Requirements (PS SoR). Volume I describes applications and services used by public safety practitioners. Its companion, Volume II, provides specific performance requirements and metrics to ensure a satisfactory quality of service level for the applications and services identified in the first volume.[33]

The PS SoR is a foundational document describing current and future requirements for the next 5 to 20 years. We'll turn to it for more detail in Chapter 6, **Conduct a Needs Analysis.**

33. U.S. Department of Homeland Security, SAFECOM Program, *Statement of Requirements for Communications and Interoperability*, Washington, D.C.: Volume I, Version 1.2, October 2006. See www.safecomprogram.gov/library/Lists/Library/Attachments/302/Statement_of_Requirements_Volume_I%20-%20Version%201_2.pdf; and U.S. Department of Homeland Security, SAFECOM Program, *Statement of Requirements for Communications and Interoperability*, Washington, D.C.: Volume II, Version 1.2, August 2008, available at www.safecomprogram.gov/library/Lists/Library/Attachments/302/Statement_of_Requirements_Volume_II%20-%20Version%201_2.pdf.

Leadership Rules

Integrating the enterprise for interoperability sounds daunting, doesn't it? It can be—and often is. The interoperability landscape is littered with a landfill's worth of acronyms camouflaging a confusing jumble of bits, bytes, megahertz, and gamma rays. Agency managers looking at the challenge of integrating a larger enterprise for interoperability often exercise the first prerogative of management: delegation!

It's a mistake, however, to allow a fascination with technology to overrun the agency's business direction. Public safety practitioners have enough problems to deal with daily without technology adding new ones. Their collective job is to deliver solutions to people in need, not carry a load of battery-powered problems along for the ride.

Corporations and other large organizations with clear visions of their missions have long grappled with the problem of technology growing to be an end in itself. They've established the roles of chief information officer (CIO) and chief technology officer (CTO) as upper-management positions with responsibility for ensuring that technology directly and measurably serves the mission. Those positions bear the responsibility of understanding the business so well that no effort is wasted in putting technology to work.

It's rare in public safety to see the CIO or CTO role formally designated by name. Whether so titled or not, the role of the person ultimately responsible for information technology, including the inseparable communications that make information sharing possible, is simple. First, it is to be focused on the organization's mission. If that person succumbs to the siren songs of technology wizards and vendors, focus is lost.

Chapter 15, **Measuring Interoperability**, delves into performance measures.

If only you could spec, buy, and install a system that ran indefinitely with a minimum of care and feeding, life would be simpler. Or at least work would be simpler. By their very nature, complex systems used for sharing information within and between public safety agencies are increasingly evolutionary. That is, they grow, changing over time. Understanding your needs is key to success.

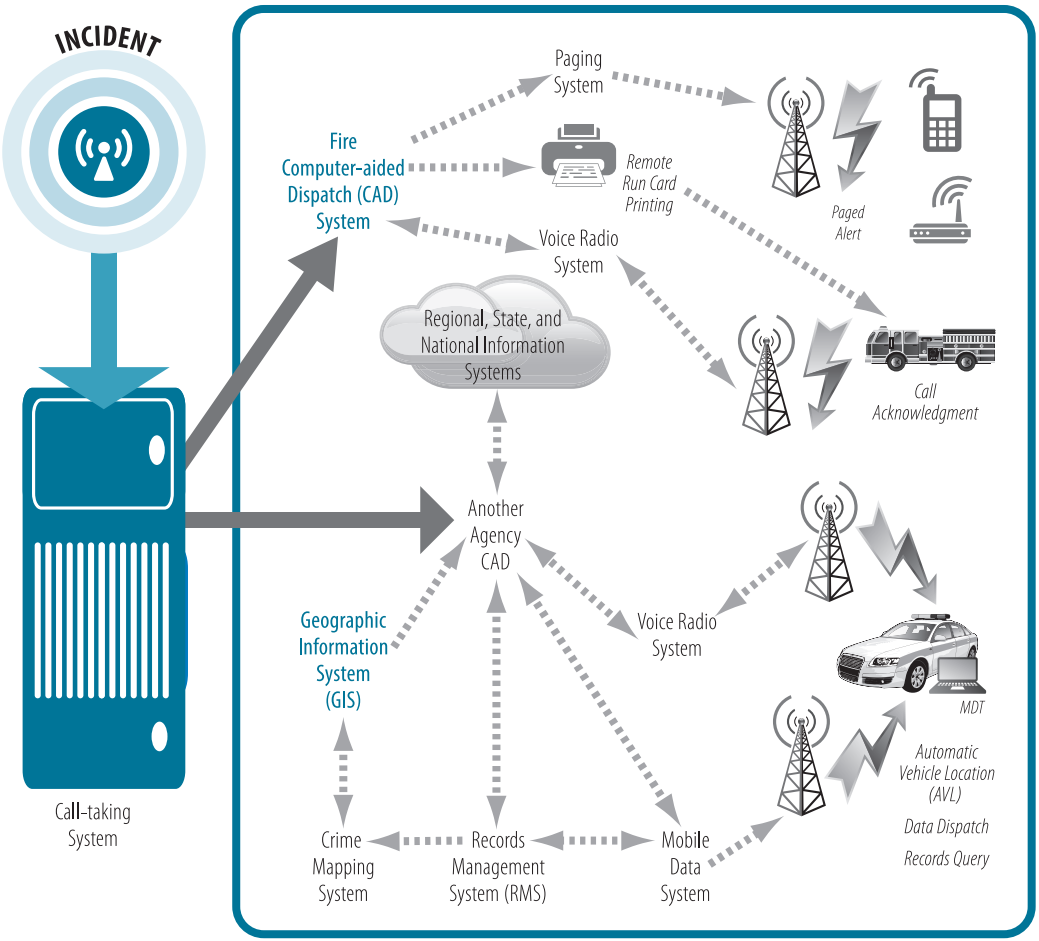
See the Big Picture

Chapter 4 of the original *Law Enforcement Tech Guide* is devoted entirely to assessing current business processes for all technology projects. In Chapter 6 of this *Communications Interoperability Tech Guide*, **Conduct a Needs Analysis**, we will provide tools specifically targeted for planning communications interoperability projects.

If all this business about integration, enterprise, and architecture seems a bit abstract when all you came to do was make sure your police, fire, and EMS agencies can talk together—well, okay, it is a bit. But consider how complex these systems can be, especially when you start lashing them together (see Figure 4-2). And consider that many big, well-funded projects have become lost in a forest of technologies because the ultimate requirements were forgotten or never even recorded.

Out of respect for our colleagues around the country, we're not going to name names—and we promise the same to you! Just don't forget the big picture. In the following chapters, we'll get into just how this elephant can be eaten one piece at a time. Step by step, interoperability can be achieved if it is built on a solid foundation.

Figure 4-2: Systems Galore



Integrated Systems at Work in 2002 Wildfire Disaster

The devastating 2002 wildfire season in the western United States included the largest in Colorado history, a blaze that threatened Denver suburbs and seriously damaged the primary watershed providing its municipal water supply. The Hayman Fire* originated in the mountains west of Colorado Springs near Lake George. It burned actively for 20 days, involved 138,000 acres, burned 132 homes, cost an estimated $28 million to suppress, and an additional $13.3 million for rehabilitation of the burn area in efforts to save the critical watershed. A U.S. Forest Service employee was implicated and later pled guilty to arson for starting the fire.

Satellite links to the Internet enabled the wireless transfer of field and planning data.

Photo courtesy of NetWest Communications Group, Inc.

© Kenneth Wyatt. www.wyattphoto.com

Geographic information systems (GIS) technology played an important part in this emergency, as it has in many wildland fires over the years. Managers of these large and often dramatic incidents rely on the graphic and analytic power of GIS for many facets of their work, from pre-incident response planning through initial and sustained attacks, and on to burn area rehabilitation.

The Hayman Fire was large and threatening enough to bring a well-equipped GIS crew in a camp trailer that operated for 18 to 24 hours a day, every day for more than 2 months. Two analysts typically worked long hours collecting data from and distributing data to field units, the incident command team, and then to outside partners who kept the public and key external decision makers informed through websites and more traditional media. A great deal of time was spent with more uncommon partners in wildland fire response, such as arson investigators, public water supply authorities, wildlife management teams, and burn area rehabilitation contractors.

A well-equipped GIS crew supported critical information sharing between field units, the incident command team, and others.

© Kenneth Wyatt. www.wyattphoto.com

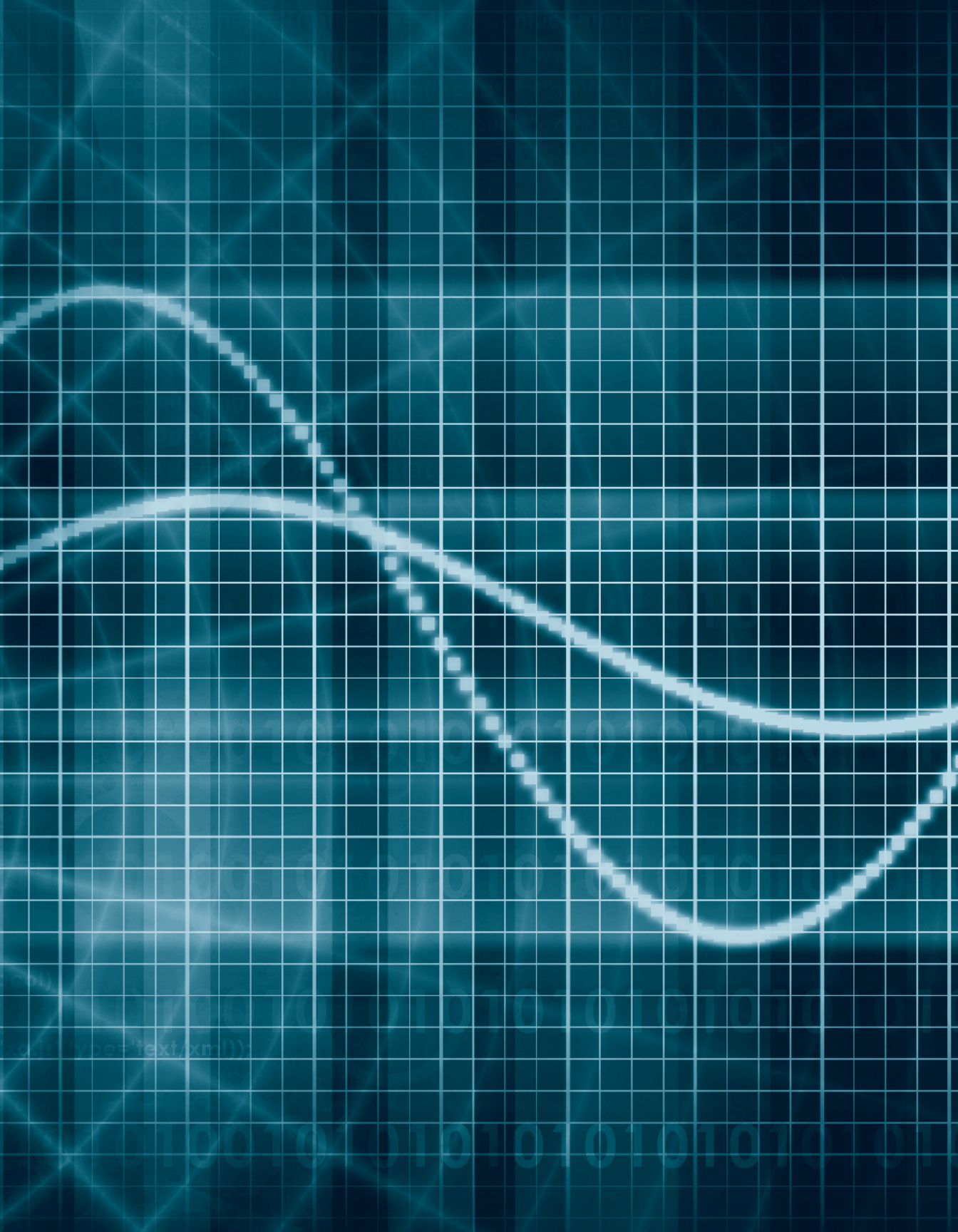
The 2002 fire season may have been the first to see bidirectional transfer of GIS data wirelessly for continuous operational purposes. According to Burn Area Evaluation and Rehabilitation (BAER) teams that worked the Hayman Fire, this was the first time that information was transferred back and forth on a daily basis to contractors for management of reseeding efforts. The fire severely damaged Denver's primary watershed, putting it at great risk from post-fire erosion sedimentation. Consequently, scarification of the incinerated watershed and reseeding was critical.

Aerial reseeding is an intensive and expensive process. The Hayman GIS trailer used its satellite link to the Internet to transfer field and planning information wirelessly to contractors who were immediately able to incorporate it into their own navigational systems for subsequent passes through the area. The power of GIS analysis, combined with an ability to transmit large amounts of information wirelessly over wideband links, allowed BAER teams to communicate in intricate detail where they needed different types of reseeding. This would not have been possible through traditional means of information sharing from remote locations.

**Note: Dan Hawkins, the author of this Guide was lead GIS specialist for 2 weeks on the Hayman Fire.*

Part 2

How is Interoperability Achieved?



CHAPTER 5

Build an Interagency Foundation

What: Communications interoperability projects and initiatives are like houses built for an extended family. They have to be built on a solid foundation, based on a decision-making structure, project management, and a charter for shaping partnerships.

Why: As with building a home, the stability and longevity of your initiative depends on a foundation of leadership, cooperation, management, and consensus, which must be built from the start.

Who: Agency executives and senior managers build these foundations. Only they can provide the leadership necessary to articulate a vision and carry out the project. They have the responsibility to set agency or jurisdiction goals and the authority to commit human and financial resources.

When: This should be done immediately, before disaster strikes or money is spent to solve an ill-defined problem. Delaying this strategic step endangers all other parts of the project.

Part 2 of this Guide is intended to provide a step-by-step process and tools for your interoperability project. This chapter and the following five chapters mirror parts of the original *Law Enforcement Tech Guide* with a specific focus on the special, often challenging, aspects of interagency communications projects. The final chapter of Part 2 offers ideas and current best practices in measuring communications interoperability that you will find useful in gauging progress toward making sure radio, computer-aided dispatch (CAD), records management systems (RMS), and other communications and information sharing systems are enabling, rather than disabling, technologies for public safety.

This chapter presumes you are starting or managing a communications interoperability initiative focused on improving the delivery of your agency's services that entail cooperating with other agencies. Your project is probably part of or influenced by larger interoperability initiatives—maybe within your own jurisdiction, but very likely in nearby ones, elsewhere across the state, and even nationally.

Build your interoperability project foundation by doing the following:

- Establishing a decision-making structure
- Hiring or assigning a project manager
- Developing a project charter

We'll deal with these step-by-step.

He who has not first laid his foundations may be able with great ability to lay them afterwards, but they will be laid with trouble to the architect and danger to the building.
—*Niccolo Machiavelli*

Projects to improve communications interoperability are fundamentally multiagency in nature. Before we get into these pieces of your project's foundation one by one, consider what's at the heart of multiagency and regional projects.

The Heart of It: Partnerships, Planning, and More Partnerships

Consider the analogy of interoperability as the house your extended family chooses to live in for everyone's mutual benefit. Now, before that scares you off, consider that economic or other necessities make this not only unavoidable, but desirable for all involved. If you were building that house, you would have to start with deciding how you are going to live with each other—setting rules of engagement, some might say. Each party's private space (jurisdiction, responsibilities) would have to be respected and accommodated. Your common space (interoperations) would have to be carefully planned to meet everyone's needs to live together without dysfunction (without disabling needed internal command, control, and communications).

Before this analogy causes you to run screaming away from your interoperability project, think what a challenge building that house would be. Think about the interagency communications challenges (and successes!) that you have today, how hard it will be to improve interoperability without partnerships and some serious planning, and the level of cooperation necessary to keep that household together long after it's built.

Interoperability is co-*operating*.

Interoperability is the ability to work together. It is conducting effective joint operations. It is co-*operating*.

Begin With the End In Mind

We've all heard Steven Covey's words of advice for being a highly effective person. One way to be highly effective in planning your communications project is to begin the project with the end of the system's life (as you know it) in mind. Life cycle planning is a cyclical process focused on continual improvement of a system. It goes beyond purchasing, installing, and operating a communications system. It is common for agencies to develop partnerships, conduct initial planning, and implement the technology, but not go any further.

Planning for the life of a communications system is just like planning for our hypothetical house to last long after the mortgage is retired. If you want the foundation, walls, plumbing, appliances, etc., to last, you plan and budget for maintenance and replacement of those things. As your family's needs change, you may update the electrical so it is more efficient, or add rooms or accessibility features. You make renovations so the house continues to meet the new or future needs of the occupants (users).

Life cycle planning doesn't mean the exact same system lasts for 20 or 30 years. If this was the case, the system would not meet the needs of the next generation of users. Life cycle planning means just the opposite. In 20 years, because the system was maintained and refreshed, it is dependable and meets the user's needs no matter that those needs may have changed. This is possible in part because practitioners and planners are better able to forecast long-term funding requirements, and help set the framework for establishing and maintaining a new or existing technology system.

Engaging in a system life cycle planning methodology, such as provided in the Office of Emergency Communications' *System Life Cycle Planning Guide*,[34] will enhance partnerships and planning efforts. By beginning your project with the life cycle in mind, you will increase your ability to accurately determine and budget project costs and provide opportunities for successful technology planning, acquisition, implementation, maintenance, refresh, and disposal over a communications system life cycle.

Foundations 101: Decision-making Structure

The decision-making structure for your interoperability project provides leadership and accountability. It defines the joint business of agencies that unite in a project to improve communications between their operations. It ensures that the project is effectively managed, and meets identified goals in a timely and cost-effective manner.

When you officially create a structure and announce it to internal and external stakeholders, you've drawn an organizational blueprint for building a house that's respective of individual agencies' roles and responsibilities, yet allows each agency the communications necessary for cooperation.

> Men often oppose a thing merely because they have had no agency in planning it, or because it may have been planned by those whom they dislike.
>
> —*Alexander Hamilton*

34. Available at www.safecomprogram.gov/library/lists/library/DispForm.aspx?ID=324. Refer to the Planning Guide for more information on this topic.

Process – Project – Process

The term "governance" is sometimes used to describe a decision-making structure. Most appropriately, governance is the body or organizational structure guiding a larger interoperability process, as opposed to a specific project. For example, a multijurisdictional region may have an overarching initiative to improve communications interoperability. Or a state may have an interoperability executive committee (SIEC). Within those processes, there may be multiple projects being undertaken by a variety of involved partners.

We use the term "decision-making structure" here specifically for projects that have an identifiable beginning and end. Governance bodies generally serve ongoing initiatives or oversee management of multiagency systems after implementation.

Processes to improve interoperability lead to projects and back to processes for managing underlying systems—organizational and technical—over their life cycles. As systems become long in the tooth, processes to improve them arise again.

Follow these six steps to create your project decision-making structure:

1. Identify Executive Sponsorship
2. Identify Stakeholders
3. Create the Structure
4. Involve Other Subject Matter Experts (these SMEs must include end users)
5. Conduct Effective Meetings
6. Decide on Project Staffing

We'll explain later in this chapter how to wrap up all the details of these steps into a document—the project charter—to record everything for posterity and make it easy to share these keys to success with others.

Step 1
Identify Executive Sponsorship

Start your project by identifying the top champion (or champions) for the initiative. This person(s) defines what the project will achieve. You may be reading this Guide because you will be that champion. Or you may be in a steering function for your own agency, but know the project will need higher leadership to bring other agencies and jurisdictions to the table. Or maybe you've already been assigned to manage the project and recognize the importance of building this part of the foundation.

Executive sponsorship is best provided by a single individual ultimately responsible for services provided by core stakeholders. In many cases, that isn't possible because interoperability projects involve multiple agencies, by definition, and often span legal jurisdictions. There either isn't a single person with such responsibility or the project has to go on without the active, ongoing support of the single individual in that role (e.g., mayor, chief county executive, chair of a regional board).

Identify three or fewer sponsors.

Ideally, sponsorship is provided by three or fewer executives. The fewer, the better, from the perspective of leadership and decision-making. With too many sponsors, political factions are more likely to arise: City versus County, Police versus Fire, etc. There's always a risk of parochial decision-making, of course, but the more people involved, the easier it is to duck responsibility for decisions. Accountability is key for sponsorship.

This begs the question of who, exactly, are the core stakeholders? There's no easy answer to that. You'll have to make that decision. Remember this: **There's a difference between sponsorship and the project's Steering Committee, which will have broader representation.**

Find sponsors with sufficient stake in the outcome to be able to lead from a position of authority, yet with the skill to draw others together. For example, we're familiar with one major city whose director of homeland security oversees both the police and fire departments, has responsibility for emergency management, and has considerable interest in EMS. This person is a strong and natural executive sponsor for that city's interoperability initiatives.

Executive sponsors communicate vision.

The executive sponsor's key role is to communicate a vision. For communications interoperability, this vision paints a picture of what success looks like when radio seamlessly connects parts of an emergency response. For every project, there is a nugget, an acorn from which everything else grows. The sponsor's main job is to regularly impart a succinct vision of success to all stakeholders.

This vision is captured in the project charter. We'll have more to say about the vision statement of your project charter near the end of this chapter.

Interoperability Summit

In early May 2005, the U.S. Department of Justice (DOJ) convened a summit on communications interoperability. Representatives from major projects and initiatives around the country came together for 2 days in Seattle to share lessons learned. Through discussion and consensus, some best practices were developed.

Sponsorship

✔ Get the right project sponsors by showing the public policy and political impact of problems to be solved.

(See www.cops.usdoj.gov/Default.asp?Item=1495 and *Perspectives on Interoperability from the Law Enforcement Community*, 2005, www.cops.usdoj.gov/pdf/Final_Seattle_Report_Summit.pdf.)

Step 2
Identify Stakeholders

The process of identifying executive sponsorship leads directly into the next step: Identify stakeholders in the effort to improve interagency communications.

The original *Law Enforcement Tech Guide* provides a discussion of the internal and external stakeholders common to technology projects of all sorts—law enforcement and otherwise. Take a look in that Guide for some stakeholders you may not have thought of!

Your early efforts to identify stakeholders and consider their role in the project will pay dividends long after switches are flipped. Some have a central role in steering the project, some define critical requirements, and others decide whether the initiative thrives or dies on the vine. This is your first step in figuring out how to keep stakeholders informed and engaged from their respective realms of interest.

Know thy stakeholders.

Typical stakeholders for communications interoperability projects include the following:

- Field operations users
- Field operations command staff
- Fire, police, and emergency medical services (EMS) chief executive officers
- Dispatch operations users
- Dispatch management
- Technical support staff
- Emergency management officials
- Elected officials
- The media
- The public

The Reluctant Stakeholder

All stakeholders are going to be equally enthusiastic about this initiative to improve their interagency communications, right? Wrong. Most projects of any size "enjoy" a range of buy-in across the wide variety of stakeholders discussed here. From the comfortably non-communicative to the incurably cynical to the painfully frugal, interoperability projects have their share of stakeholders who won't wildly embrace change.

It's a big mistake to proceed by simply labeling these folks, pigeonholing them, and stacking committees with cheerleaders. We see this most frequently where a "solution" arises before problems are well understood.

By bringing dissenters to the table, issues get aired and the group—as a whole—can make the commitment to move forward. Even those whose ideas or objections were considered and decided against have to acknowledge that a deliberative, consensual process delivered the results. Often enough, these folks understand real challenges that need to be faced.

A good project manager can use the art of facilitation to move stakeholders from simply reacting, to problem solving, and on to creative choices.

Unfortunately, nothing can guarantee the transformation of the reluctant stakeholder into a productive project team member. A knowledgeable project manager will have project communications and risk management plans in place to mitigate the potential effects of a reluctant stakeholder.

We've heard from more than one region where organized labor groups were ignored as stakeholders—to the great detriment of the project. By contrast, we've also heard success stories where labor has been central in identifying needs **and** managing expectations—both of which are definite keys to project success!

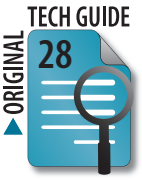
The last two groups are increasingly identified as stakeholders. The profile and cost of communications projects, in general, has grown dramatically and public attention to interoperability problems is at an all-time high. Critical media attention is increasingly drawn to costly public technology failures, further influencing public perceptions. Less commonly recognized is the growing opposition to new radio towers. The first time you plan to erect a new one in a residential neighborhood, you'll learn about new stakeholders!

Plan to communicate with the public and media.

Including the media and public in plans to honestly communicate the project's goals, successes, and even failures is important to any high-profile project. Consider including representatives of each as ex officio members of your committees.

If two men agree on everything, you may be sure that one of them is doing the thinking.
—*Lyndon B. Johnson*

Step 3
Create the Structure



The time has come to formalize your project's decision-making structure. Doing so and making it widely known ensures all involved will know where responsibility and authority falls. Leadership and accountability roles are made clear, as are reporting roles.

Figure 5-1 on page 81 is a typical structure for multiagency, multijurisdictional efforts. The different elements are discussed in detail in the original *Law Enforcement Tech Guide*, but we'll cover some twists common to communications interoperability projects.

Steering Committee missteps with vendors can be costly—or worse.

With executive sponsorship in place, a Steering Committee can begin to take form. Multiagency steering committees are like police interceptors or firefighting helicopters: They are high-performance tools that can lead to trouble if misused. Like any committee, the mix of members and their individual talents determine how well work proceeds. Members must have the authority to commit resources and the ability to work collaboratively. They must be strategic thinkers and comfortable managing the work of others. Ideally, Steering Committee members are adept with large procurements or can be made so through early committee work.

Project management is the next piece of your decision-making structure. It is such a critical piece; we'll talk about it in detail shortly.

The final pieces depicted in the chart are two important working bodies—the User Committee and the Technical Committee—and perhaps several topic-focused work groups that will be created to address particular tasks and dissolved when they're no longer needed.

Users know best.

The User (or operational) Committee is made up of stakeholders familiar with the business and operations of the agencies they represent. Some of the most effective committee members are line supervisors and managers of dispatch and field resources. A shift supervisor, district sergeant, or fire company commander is generally better in tune with the intra- and interagency radio communications needs of their organization than anyone else. In some cases, individual dispatchers, officers, firefighters, and paramedics may have to translate their own experience to broader operational needs.

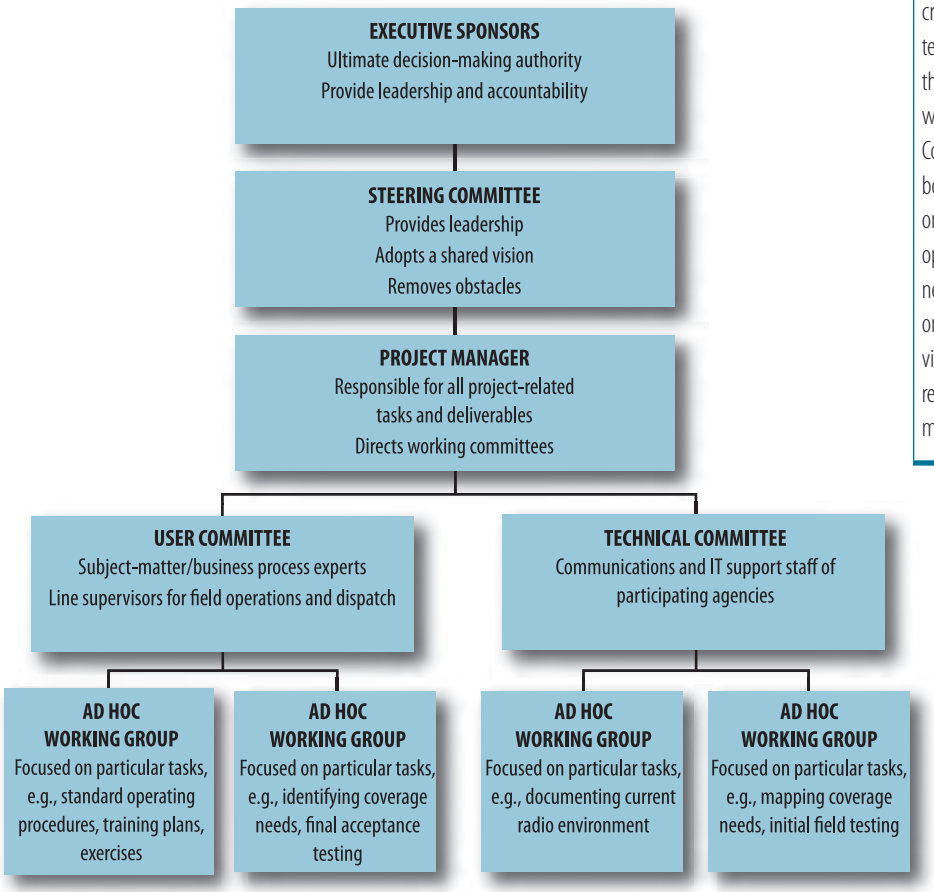
The Technical Committee is charged with taking the project's vision, folding in operational needs, and analyzing the current technical environment. Potential solutions may be examined to craft technical requirements for eventual procurement. Involving technology specialists and information technology (IT) staff early on can reduce costs by leveraging existing intra- and interagency resources to create a system that is more reliable. Here, most of all, "requirements tunnel vision" has to be avoided because it can easily produce restrictive requirements that slip through into procurement documents, leading to bid protests about foregone conclusions.

Avoid attention creep!

We'll discuss how to focus working committees and further flesh out their roles in Chapters 6, **Conduct a Needs Analysis**, and Chapter 7, **Create a Project Plan**.

A classic sign of attention creep in radio projects is technology debates in the User Committee—or worse yet, in the Steering Committee. The former body should be focused on defining the project's operational and business needs, and the latter on executing a shared vision, committing resources, and top-down management.

Figure 5-1: Sample Decision-Making Structure



A caveat: Remember that each element of the decision-making structure has its own role, expertise, and responsibilities. Resist the idea that, for example, the Steering Committee collectively knows more about operations and technology than the working committees formed to address those issues. Use the decision-making structure to delegate responsibility and concentrate each group's attention on its own role.

Interoperability Summit

More notes from the U.S. DOJ Interoperability Summit

Decision-making Structure

- Ensure committee members have authority to speak for their agencies.
- Get buy-in from labor unions and ask them to recommend their own representatives.
- Manage competing stakeholder demands between larger and smaller agencies by creating a balanced decision-making structure with documented conflict resolution processes.

Step 4
Involve Other Subject Matter Experts

Outside subject matter experts can be involved in your decision-making structure at several levels. Some ideas:

- Bring in organizational and strategic management experts early on to sit down with your Steering Committee and get it started on the right foot.
- Ask representatives from outside projects or interoperability initiatives to address steering and working committee meetings.
- Rely on legal and procurement expertise within your agencies or elsewhere in government to keep your project out of trouble. If grant money is being utilized, make sure that local procurement policies are consistent with grant guidance.
- Have incident management specialists work with your User Committee to define interagency communications needs in terms consistent with the National Incident Management System (NIMS) and its Incident Command System (ICS).
- Use technology experts to help your Technical Committee frame available opportunities to use or extend existing infrastructure.

Consider the range of expertise that may be brought to bear on your project. You may have to hire new staff in some areas, but will likely find internal staff nearby who are involved in related projects and available to assist with yours. For example, organizational and project management expertise might be available within your stakeholder agencies or others outside of the project, such as other units of government. Help might also be available at no cost through federal assistance programs for public safety agencies.

Use free technical assistance resources.

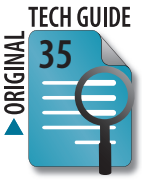
Nationally, both the U.S. Departments of Justice and Homeland Security maintain assistance programs that can provide help at no cost. If your project will receive grant funding, talk with your assigned grant specialist for guidance on assistance that may be specifically available under the funding program.

Some of these programs bring peers together for training. Whether you're in a project sponsorship, management, or technical role, recognize that the opportunity to network with your peers can be tremendously valuable. There are others who may have faced and overcome challenges you're up against right now. Some of the best and least expensive subject matter expertise available to your project can come from peers in other jurisdictions. Take advantage of this broad and inexpensive resource. Consider asking them to address your committee meetings and share experiences.

Network with peers.

Step 5

Conduct Effective Meetings



Meetings are inevitable, so you might as well make them effective. "Fun" meetings are something of an oxymoron, but there are ways to make them less dreadful. Food and refreshments always work, as do pleasant surroundings with plenty of space and good acoustics so people don't struggle or become uncomfortable while helping the project move forward.

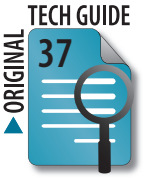
The key to good meetings is organization and brevity. People resent their time being wasted and know intuitively when it's happening. Consider using a trained meeting facilitator during initial group meetings to get them started on the right foot. If you're the project manager, work carefully with the facilitator so they know your goals, process, and group dynamics. Observe carefully and learn what you can do to make future meetings effective.

Use a trained facilitator early on.

The original *Law Enforcement Tech Guide* provides some great tips for keeping your project on track by making the most of the inevitable meetings that most everyone dreads. These are rules that can be used in projects of all types.

Step 6

Decide on Project Staffing



The last step in establishing your project's decision-making structure is one of the toughest: decide how the project will be staffed and where resources are going to come from. Once again, the original *Law Enforcement Tech Guide* provides most of what you need to know about staffing your technology project—whether it's for communications interoperability, voice or data, or even for technology far outside the law enforcement business.

The bottom line is this: don't handicap your project—or worse—by ignoring the fact that managing an interoperability project of most any size is a lot of work! Multimillion-dollar communications projects are becoming increasingly common. When the first edition of this guide was written, one large, populous western state was considering building a multiagency communications system estimated to cost $5 billion. Project staffing for such a project would be immense!

Consider this rule of thumb: consulting services, including project management, will commonly take 10–15 percent of a technology project's budget. Consider both how much organizational, process, and technical expertise you'll need for this project and how much you have at hand. If you have all the expertise internally that will be needed, recognize that while you may not be spending that 10–15 percent, you will be taking resources worth that much from elsewhere in the agencies.

Plan accordingly. Staff the project appropriately. Resist the temptation to save that 10 percent for more radios, sacrificing good management of all resources in the process.

Foundations 102: Project Management

> "Management" means, in the last analysis, the substitution of thought for brawn and muscle, of knowledge for folklore and superstition, and of cooperation for force. . .
> —*Peter F. Drucker*

Our discussion of project staffing leads to the next key ingredient of the project foundation mixture—project management.

The choice is simple: you have to hire, assign, or train somebody to be the project manager. If the project will cost more than a few hundred thousand dollars, your practical choices are reduced to hiring an existing, experienced project manager or assigning one from within participating agencies. **Assign inexperienced staff in larger projects at your own risk.**

No single person or function in a project has the potential to make or break success like the project manager. Because this person is a single point of coordination between upper management, all work being done, and vendors, the project manager has great responsibility. The best project managers have an uncommon combination of business process, management, operations, procurement, and technical skills. Combined with distinct project management skills, they have the uncanny ability to assume temporary ownership of results, while delivering permanent ownership of final products to stakeholders.

Good project managers make things happen, but don't usurp the roles of others in the decision-making structure.

The project manager's responsibilities, skills, and personal attributes are well addressed in the original *Law Enforcement Tech Guide*. Use that Guide as a practical tool regarding all the project manager's responsibilities in a public safety technology project.

Communications interoperability projects may be some of the most difficult to manage. They are typically:

- Large, expensive projects
- Inherently multiagency in nature, bringing inevitable conflict and compromise
- Critical to the delivery of core services affecting life and death
- Built using a variety of complex technologies
- Involve civil construction and permitting
- Require environmental, historical, and cultural assessments for sites

Smaller jurisdictions, as a group, are slowest to hire or assign full-time project management. While other technology projects are often proportional to the size of the agency, radio projects generally aren't. For example, a computer-aided dispatch system is simpler for a small agency than larger ones, requiring less project management. Radio projects, on the other hand, are generally large and expensive—even for smaller jurisdictions. For specific guidance on small and rural agencies, you may want to refer to the *Law Enforcement Tech Guide for Small and Rural Police Agencies* found at http://ric-zai-inc.com/Publications/cops-p086-pub.pdf.

- Completely dependent on federal licenses and permits for frequencies and towers
- At risk of planned (and unplanned!) obsolescence

If you're in an executive sponsorship or steering role, do yourself a favor and hire or assign someone full time to manage the project if it's much more than an effort costing a few hundred thousand dollars. **Don't make the mistake of figuring that project management is a sideline job for someone with other responsibilities.** That's a sure road to failure. A full-time assignment will get the job done better and faster.

Foundations 103: Project Charter

Okay! To return to our analogy—you have lined up the designers, architects, foremen, and eventual occupants of this house for an extended, interoperable family. Now it's time to create an architectural drawing of what it will look like.

The project charter is the single most important document you can create for your interoperability project. It is a written document presenting a vision of what is to be accomplished, defining scope, goals, and objectives. It includes a description of the decision-making structure to be used, project management approach, and initial resource requirements. Plan to distribute it widely after approval by the project's executive sponsors and have it used by all members of the project. Typically, it's put together by the project manager and Steering Committee with input from working committees, if they've been formed.

The original *Law Enforcement Tech Guide* covers development of a charter in detail. We're not going to recreate that wheel here, but we do want to touch on a couple of high points, with special applicability to interagency and communications projects.

The original Guide also provides a 12-step Program for creating the charter. The steps are:

1. Write the Vision Statement
2. Give the Project a Name
3. Get the Big Picture, Conduct an Environmental Scan
4. Build the Business Case
5. Include Background or Historical Information, if Relevant
6. Establish the Project Scope
7. Establish Preliminary Project Objectives

8. Note Major Project Assumptions and Constraints
9. Develop Initial Timelines and Preliminary Budget
10. Include Project Planning Methodology
11. Provide Project Team Organizational Chart and Membership Roster
12. Sign, Seal, and Deliver

Don't get your charters confused. Governance charters serve to coordinate governance bodies overseeing ongoing initiatives. Project charters authorize and acknowledge a specific project that the governing body oversees. Both play a critical role in successful interagency technology initiatives. For example, let's say a number of municipalities decide they want to implement a regional CAD/RMS. As part of building their foundation, in addition to the necessary local-to-local memorandums of understanding (MOU), the stakeholders create and sign a governance charter to oversee the decision-making organization of the regional system beyond the project life cycle. To formally authorize and recognize the regional CAD/RMS project itself, the chartered governance mechanism creates a project charter, complete with its own unique decision-making structure. Unlike the governance charter, the project charter is only in effect for the life cycle of the CAD/RMS project.[35]

The **vision statement** may be crafted entirely from scratch, or it may be provided to the Steering Committee by the executive sponsors or even by some larger planning process outside this project. For example, the vision may come from a homeland security or technology strategic plan describing the need for the project. It may come from legislation, decree, or interoperability coordination bodies at the regional or state level.

Adoption of a **project name** is an opportunity to develop some teamwork within the Steering Committee. A simple, descriptive name provides an easy way to identify the initiative. This provides a "brand" inside and outside the project. Some have even had a bit of fun with it.

> Interoperability is all about relationships and working toward a common vision. Perhaps the first step in 'breaking the ice' might be to collectively develop a catchy acronym, such as DIRT (Disaster Interoperable Response Techno-communications).
>
> — Chief Charles Werner
> Charlottesville (Virginia) Fire Department

35. SAFECOM has developed a suite of templates to assist agencies with developing interagency charters, memorandums of understanding, and other formal agreement documents. See www.safecomprogram.gov/oecguidancedocuments/webpages/ts.aspx.

The **environment scan** is a process more unfamiliar in name than practice to folks outside of the project management business. We've touched on the fact that your project is probably affected by other projects going on in nearby jurisdictions. Your project will be planned and executed in context with other technology, interoperability, management, and operational changes taking place around you. For example, your jurisdiction may have a related project underway to build a microwave backbone to carry all forms of information for agencies, including audio and control signaling for radio systems. You should certainly be aware of that initiative in your own initial planning.

Plan in context.

Building the **business case** is often difficult for public safety practitioners unaccustomed to marketing ideas and products. It's easy to describe the need for new technology in dire terms of apocalyptic proportions. Or conversely, to promise World Peace and Eternal Harmony between police, fire, and EMS agencies. That sounds a lot more like a charity pitch than a business case. Resist if you find yourself writing, "If it saves one life, it's worth the millions of dollars." While a worthy sentiment, such hyperbole doesn't help explain why *this* project and *that* amount of money will make a difference.

Explain the operational benefits to be achieved in specific terms.

Explain the operational benefits to be achieved in specific terms. For example, "A new shared radio system will support consolidated incident action planning necessary during events involving six or more police, fire, and EMS units, as well as avoid estimated replacement costs of $13 million for each of the three separate radio systems over the next 5 years."

Scope: What's in, what's out?

Relevant **background or historical information** is easy to find for most radio communications projects since most systems have been used by generations of responders. There's usually good background on how the involved agencies ended up with the systems they currently have and how interoperability problems arose. Remember that the goal in this portion of the project charter is to explain how this project came about.

In creating the charter, the team has its first opportunity to establish the **project scope**. It's fairly general at this point, but should clearly define what's in and what's out of the project. For radio systems, relevant factors to describe are involved agencies, whether the project replaces existing capabilities and/or provides new ones, and the geographic area to be affected. We'll have more to say on scope planning in Chapter 7, **Create a Project Plan.**

Focus on operational outcomes, not technology.

Project objectives have to be specific and measurable, so take time with the Steering Committee and User Committee, if it's in place, to identify key objectives that can be quantified and measured for completion. As with the business case, remember these are being written with others in mind—both internal and external stakeholders. Since you're planning to improve communications interoperability, take time to describe the "who, when, where, and what" of new interagency capabilities. Be specific. Focus on operational outcomes—not technology. For instance in this example, "Provide all police officers across the county with a communications channel that is immediately available for coordinating pursuits at all times," there are many ways to meet this objective, but the "how" is left for later determination.

Project assumptions and constraints should be documented to explicitly note for all team members and stakeholders what is expected, not only of them, but conditions under which the project may have to take one turn or another. This is an important part of your charter because it captures conditions participants tend to forget—but which shaped the project. For example, if the project is to create different degrees of interoperability over time or between different partners in phases based on available funding, do the best you can to identify priorities and contingencies. Similarly, your project may move faster, slower, or not at all based on continued funding under special revenue programs. This section is the best place to state assumed contributions by cooperating agencies to ongoing systems operations and maintenance.

Everyone wants to know how long it's going to take and how much it's going to cost.

Initial timelines and preliminary budgets are specific, central assumptions and constraints placed on the project. Unlike the preceding section, these may be mainly a matter of choice between participants. Take the opportunity to put a stake in the sand to describe these key components of project management.

Your **project planning methodology** may still be in development as the charter is developed, but include plans for steps that will be taken along the way to improving interagency communications through this project. How will needs be assessed? How will progress be communicated to stakeholders? When will a project plan be developed? Large and costly interoperability projects will likely require outside expertise in one or more steps along the way. What will be done internally and what will be outsourced?

The **project organizational chart and roster** find their first formal home in this document. Accept that they will change over time and commit to keeping this portion of the charter up-to-date.

The final step is to **sign, seal, and deliver** the charter. Typically, sponsors and Steering Committee members sign the charter. Don't be shy about distributing the finished charter to stakeholders everywhere.

Footings on Bedrock

A good home must be made, not bought.
—*Joyce Maynard*

Follow these steps and your interagency project will have a foundation with footings on bedrock. You'll have a decision-making structure that reinforces roles and responsibilities while accommodating the variety of needs brought to the table. Your project manager—maybe you—will have the necessary room to work and resources to accomplish this most important task. A project charter captures all these initial operating details and much more.

Altogether, this foundation will provide much more than just the basis for a successful project: it may be the foundation for better interagency communications.

The extended family may not be ready to move in yet, but you know they're coming! Read on.

CHAPTER 6

Conduct a Needs Analysis

What: A needs analysis is the organized process of collecting information on what's happening today, the technological environment in which it happens, supported and unsupported needs, and generally what's required of an interoperable system.

Why: Since communications interoperability is achieved through a system of systems—both technological and operational—needs are many and varied. Project success pivots on meeting well understood and defined needs. Needs analysis feeds acquisition, implementation, maintenance, and most other system development efforts.

Who: The project manager is primarily responsible for needs analysis. The User and Technical Committees define operational needs and the current technological environment.

When: As soon as a decision-making structure and a charter are in place, but before preconceived, often competing, notions of solutions start to build fan clubs, a needs analysis can proceed in parallel with creation of a project plan.

Needs analysis provides the means to link measurable outcomes to the use of technology. It combines a structured process to define operational requirements with an interactive one to build stakeholder involvement. The products of this phase of your project prove their value in operational terms.

Chapters 4–7 of the original *Law Enforcement Tech Guide* deal with needs analysis for technology projects in general.

Your project to improve communications interoperability is well underway. It has the necessary foundation for decision-making and stakeholder ownership. It has the project management in place that's needed to keep efforts focused. And it has a semi-formal agreement—the charter—to assure a clear strategy for what is to be accomplished. The next step is to delve into the details of what your project will accomplish—The Needs Analysis.

Public safety agencies don't need radios. They need the operational capabilities generally and historically supported through wireless communications. This might seem like a play on words, but too often a focus on the means of meeting a functional need puts requirements, themselves, out of focus. This is a common pitfall in using technology of all sorts, not just radio.

The need for interoperability is widely recognized today. Unfortunately, once past the sound bites and impassioned speeches, agency leaders are left with the more difficult task of coming up with more than just interoperability: they need interoperations.

Needs analysis details what has to be accomplished to achieve interoperability.

Since emergency response is the business of public safety, the business case for interoperability today describes why police, fire, EMS, and other agencies have to communicate with one another and what the "costs" are when it's done poorly. A needs analysis details what is necessary to meet the project charter's business case. It describes exactly what has to be accomplished for interoperability to be achieved.

Conduct your interoperability needs analysis using the following steps:

- Assess current business processes
- Determine stakeholder needs
- Develop general system requirements
- Evaluate *buy* versus *build* options

Development and design of shared systems follow the same interagency processes described here, though necessarily with more time spent in understanding each agency's internal processes, collecting their needs, and finding common requirements. User and technical committees for such development efforts should use ad hoc work groups from each participating agency to develop requirements that can be rolled up for system wide needs analysis.

Whether your project is simply to improve interoperability among users of existing systems or to build a broad, new shared system, understanding communications needs between agencies requires the specially focused efforts detailed here.

Needs Analysis 101: Assess Current Business Processes

Needs analysis begins with an assessment of current business processes. Often we work together, but have no formal statements of how that will happen in detail sufficient to plan complex systems. Complexity is managed by breaking the problem down into small pieces (see Figure 6-1). This is how a business process assessment is done.

It is impossible to design a system so perfect that no one needs to be good.
—*T.S. Eliot*

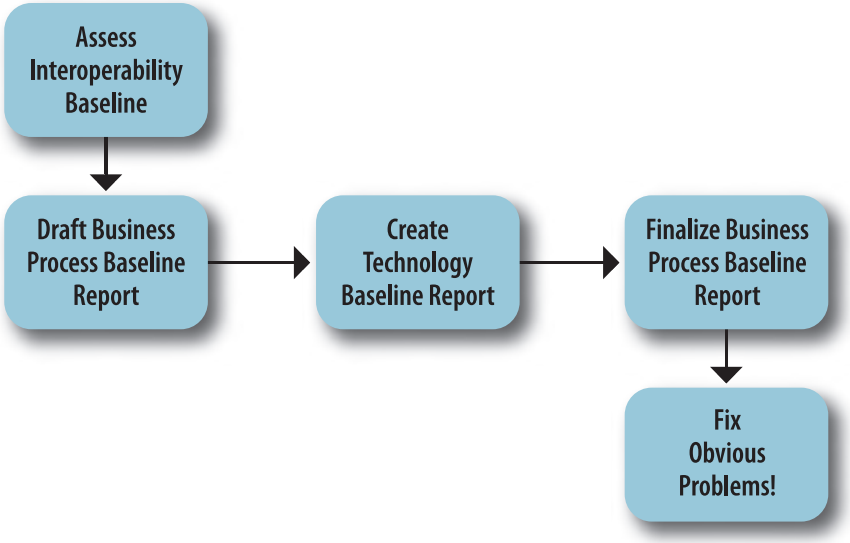
Working committees are key to completing a good assessment. Both User and Technical Committees have reams of information to provide from their respective perspectives that has to be captured. The results of their work feed the next phases of needs analysis—and the project well beyond.

Keep the committees focused on their roles. The User Committee represents *operational* expertise. It must define the business processes that make interoperability so critical. Don't let it stray into the realm of *technology*—the Technical Committee's specific area of expertise. Resist the temptation to see interoperability as primarily a technical problem; it isn't. The User Committee must have ownership of the operational needs and requirements for interoperability.

Working committees are key to a good assessment.

Your business process assessment will be an iterative process. That is, draft reports will generate further important information that should be incorporated. Not only will new bits of information arise step by step, but mistakes will be discovered that need to be corrected.

Figure 6-1: Business Process Assessment Steps



Conduct the assessment accordingly, keeping draft reports, diagrams, charts, and maps in front of the project decision-making structure for the very purpose of getting details accurate and complete.

Step 0
Assess the Interoperability Baseline

As the project manager, you can get started with real needs analysis by assessing the existing state of interoperability among project partners. This interoperability baseline assessment provides a snapshot for future comparison. It's an entirely optional step that can serve as a useful tool to start subsequent conversations.

Use a stake in the sand to draw feedback.

Chapter 15, **Measuring Interoperability**, describes a method for conducting an interoperability baseline assessment. Read and follow the process described there if you choose to kick off your needs analysis with one. It shouldn't take more than an hour or two to complete, at the most. The objective is not to conduct a scientific study, but to have a stake in the sand to draw feedback about the state of interoperability in your project area. The assessment can be used with the Steering Committee and all working committees to frame issues, elicit feedback, and achieve some consensus on challenges faced.

For diplomatic purposes, assess interoperability *up to* the start of this project; measures of leadership and governance of your current project, among other things, are yet to be proven!

Step 1
Define Interagency Business Processes

The first formal step in analyzing needs is to define regular, authorized, planned, or otherwise existing interagency response processes that are already in place. Start by collecting interagency standard operating procedures (SOPs) that describe how partners plan to or already work together. These describe interagency business processes.

With existing SOPs in hand, it's time to convene the User Committee and have it define processes requiring communications between agencies. If interagency SOP pickings are slim, the User Committee may be the only place you'll find out just what interoperations are currently being enabled by communications.

We'll talk about techniques for collecting stakeholder needs shortly. Some detective work may be necessary to discover business processes that must be supported by current and future communications systems—particularly undocumented ones.

Unwritten business processes are important to document.

For example, there may be a general, but unwritten, practice that police units respond to structure fires of a certain size for traffic control. Or, quick response units from two jurisdictions are automatically dispatched to injury accidents on a bridge spanning them. These are interagency processes, perhaps coordinated through a mutual dispatch channel or common tactical talkgroup.

Even if unofficial, existing business processes *must* be documented.

☐ Product: A Draft Business Process Baseline Report

Business processes are documented in a report describing the "who, what, when, why, where, and how much" of interagency communications. This describes work that agencies do together. It's the "as-is" of your business processes. Leave the "how" for the next report on the technical environment.

Use diagrams to make work models clear.

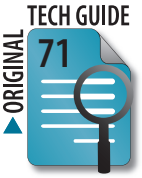
The project manager is responsible for producing this report. Plan to release one or more complete drafts and distribute to all stakeholders. Seeing conversations rolled up into a summary report intended to describe all relevant business processes will certainly produce comments and corrections. It's important to have a draft report complete enough to be readable and understandable, but make sure everyone knows it is a draft. Emphasize that this is an iterative process and feedback will be incorporated.

Make special note of physical, electronic, and procedural security processes. Increasing threats and technological complexity call for attention to be paid to the security of communications resources, as well as to information exchanged through them. In 2007 the Program Manager for the Information Sharing Environment (PM-ISE) developed the National Security Strategy for Information Sharing. The PM-ISE helps federal, state, local, and tribal agencies stay informed of current issues concerning the security of communications and information sharing systems.[36]

36. For more information on the ISE and the National Security Strategy for Information Sharing, see www.ise.gov.

Use diagrams to make work processes more understandable. They are key to depicting work. Two types of diagrams are particularly useful:

- **Sequence work models** show processes, subprocesses, and activities. The original *Law Enforcement Tech Guide* uses sequence work models for report filing and suspect booking processes.
- **Flow work models** show information flows from person to person, organization to organization, or function to function. For example, the original *Law Enforcement Tech Guide* uses such a model to depict information flowing from dispatch to a sergeant and on to several officers.



Not only do these work models graphically depict business processes for needs analysis, they will be useful later in your project for describing functional requirements, creating acceptance tests, developing training and exercises, and for assessing the impacts of system outages. Design, implementation, operations, and maintenance stages of your project all benefit from accurate assessment and depiction of work models.

Step 2
Define the Current Technology Environment

Draft business process materials will be useful in the next step: defining the technical communications environment that enables interagency work. Typically, the Technical Committee is charged with collecting the variety of information about technology currently in use. The project manager is again responsible for collecting the information and presenting it in a form suitable for distribution.

An example of information collected for a radio system project may include:

- A matrix showing existing means of interagency communications. List all agencies on both the side and top, with each cell indicating how communications occur. Use the five *Interoperability Continuum* technology categories to characterize how communications between each pairing of agencies occurs today. The standard categorized approaches are: Swap Radios, Gateway, Shared Channels, Proprietary or Standards-based Shared System.

- General descriptions of radio systems in use by jurisdiction and agency for both voice and data. As a hypothetical example,

  "Northland County uses an 800 MHz trunked radio system for all police, fire, and EMS voice communications. Information from a common mobile data system is carried by commercial services from Horizon Wireless."

- An inventory of responder radio equipment owned by participating agencies. This information can be detailed. Summarize it in reports, but put details such as make, model, and frequency band into appendixes that can be referenced when needed.
- An inventory of supporting infrastructure, including:
  - Detailed descriptions of radio systems in use listed by jurisdiction and agency, for both voice and data
  - Caches of radios to be swapped between agencies
  - Gateways that connect voice radio audio or mobile data switches
  - Shared channels (frequencies)
  - Established interagency talkgroups
  - Radio sites (location, ownership, size, current occupants, available space, primary and backup power, receive and transmit frequencies in use, etc.)
  - Physical and electronic security measures
  - Wired and wireless backbone interconnecting parts of various systems, with particular emphasis on parts shared between agencies
  - Commercial services (vendor, capabilities, cost, availability by area)
  - Radio coverage (footprints of existing systems)
  - Technician services either available internally or contracted

This collection of information is not only important for your needs analysis, but also will be invaluable in the likely event that your project leads to procurement of additional technology.

☐ Product: A Technology Baseline Report

The technology baseline report is produced by the project manager through heavy contributions from the Technical Committee. It's important to capture all the detail described above, yet present it in summary at the front of the report.

Simple explanations of "how" are indispensable.

Remember that "how" questions can be answered in varying levels of detail. Provide the simplest one first. Again, use diagrams and charts to make information more understandable. Because of the geographic nature of communications systems, maps are an effective means of getting much of this information across, too.

Step 3
Fix the (Newly) Obvious Problems

Take advantage of quick fixes for momentum.

As mentioned, developing a better understanding of business processes often suggests immediate fixes that could be made. They may be fixes to processes and procedures or simply a way to use some existing technology more fully. Take advantage of these opportunities for improvement, but keep up the momentum with your needs analysis. Properly done, quick fixes can actually help generate enthusiasm for the next steps.

More often than not, multiple stakeholders will have an interest in even these relatively painless quick fixes. Be sure to include them in discussion of recommendations. If the Steering Committee expects to approve such changes, be prepared when presenting recommendations to request and justify resources necessary to make the changes.

Typical quick-fix examples we've seen include changes to dispatch procedures to announce staging area channels during multiagency incidents, new automatic aid agreements or formalization of existing practices, and consolidation of radio system components in shared sites. For the sake of progress, avoid changes that will take more than a week or two to implement, however. Carefully evaluate what constitutes a quick fix, leaving anything more involved for inclusion in your functional requirements and the formal project plan.

Upon completion of these quick fixes, initiate the practice of celebrating milestones along your path to communications interoperability. This is a great time to start a habit of taking advantage of visible steps of progress. A small ceremony of thanks to key participants and even press releases to claim your project's success more publicly are good moves that help to boost morale and build momentum.

Step 4

Describe How Current Technology is Used to Accomplish Work

With the technology baseline in hand and quick fixes complete, the business process baseline can now be finalized. Get the Technical Committee's assistance to take descriptions of interagency processes and add simple "how" statements. For example:

"Midland City FD and Stillwater RFD have an automatic aid agreement for structure fires in the Norwalk Subdivision. This typically requires one channel of common communications for command coordination and another between the command post and staging areas. VHF-high band shared channels are used directly between responders."

"Midland City PD and State Highway Patrol units are jointly dispatched to injury accidents on I-5 within the city limits. The PD uses a dedicated channel on its UHF conventional system to talk to SHP on its Division 1 operations channel—a 150 MHz conventional repeater—connected by a permanent gateway operated by the city."

☐ Product: A Final Business Process Baseline Report

Complete your assessment of current business processes by finalizing the baseline report. This report captures both operational processes and details of the technologies currently supporting them. If you completed one, the interoperability baseline assessment should be included, along with any adjustments due to feedback received along the way.

This **as-is report** is very important for needs analysis. As the title states, it is the baseline describing what you have today in the way of interagency operations and how communications support them. It's not uncommon in this process to run across immediate changes that could be made to improve operations. Take advantage of these opportunities by including them as recommendations in the final baseline report.

This is your *as-is* report.

Depending on your governance structure, the Steering Committee may wish to review the report before adopting it as final. It's great to have that level of support, but make sure to take into account the added time needed for review, changes, and approval when creating the project plan.

Needs Analysis 102: Determine Stakeholder Needs

You have the *as-is*. Now you can move on to the *to-be*. Project buy-in hinges on how well stakeholder needs are determined. The project manager guides this process, meeting with stakeholders at all levels, across all agencies.

A human being has a natural desire to have more of a good thing than he needs.
—*Mark Twain*

Start the process of collecting needs shortly after documenting business processes and the technology environment. This takes advantage of any momentum created and captures ideas that arose in discussing things the way they are.

While baseline assessments can be conducted relatively quickly through efforts of the working committees, collecting information on stakeholder needs requires that time be spent with a lot more people across essentially all agencies—and probably among various groups within each.

The Goals

Goal #1: Capture operational needs.

There are several goals to be achieved in collecting stakeholder needs. The obvious one is to obtain a better understanding of interagency communications needs. Often these needs are camouflaged behind ideas about how best to resolve them. While the solution to a given problem may revolve around new or innovative uses of technology, technology isn't ever the need. Work to capture the interagency operational needs to assure success and the ability to accurately recognize those needs.

A secondary, but equally important, goal is to open organizational and management lines of communications about needs. Often these needs aren't new and have had some time to "mature."

Goal #2: Open lines of communications.

Can we talk? Many interoperability problems masquerade as technical problems when in reality they're organizational or management dysfunctions—or originated there and now really are technical problems. More than one agency has built a new radio, computer-aided dispatch, or records management system without regard to compatibility with neighbors. They reduced interoperability by introducing incompatible technology, not seeing a need for interagency communications at the time.

The fact that your project is progressing proves agencies are willing to move beyond organizational dysfunctions, if they ever existed. The best way to pave over those potholes is to focus on the operational or functional needs of participating agencies. Get input not only on how they can communicate better with their partners, but also how organizational change will flow from better interagency communications.

Goal #3: Get invested stakeholders.

The final goal is to get all stakeholders involved in the process and invested in creating solutions. This occurs when they're involved in defining requirements and recognize that the outcomes will address their operational needs. Also, consider partners like the state. This will allow initiatives such as statewide communications interoperability plans (SCIP) development and state justice information systems to involve all stakeholders.

Techniques

As we're alluding to, the project manager or other facilitator's challenge in collecting needs often amounts to digging through surface layers to reach underlying needs. It's really not all that hard to do. What's tough is doing it without losing stakeholder confidence and buy-in along the way! The project manager's communications skills—and we don't mean the radio—are going to make or break this share of the project.

Objectivity is one of the project manager's sharpest tools at this point. It yields the credibility necessary to elicit honest statements of need and facilitate discussion. If you're in that role, recognize that your pre-conceived notions will be picked up from far away. Guard your credibility by remaining objective!

☐ Be Prepared: Collect Artifacts

Before going to stakeholders to solicit the needs that will shape your interoperability project, search for materials from the involved jurisdictions that may already document what those needs are. Likely sources may turn up artifacts establishing de facto requirements, stating unmet needs, or otherwise exposing interoperability holes. Formal or anecdotal, these artifacts are invaluable in exposing stakeholder needs.

The business process baseline often highlights a number of these artifacts, and commonly draws attention to neglected or unnecessary ones. Other likely sources include:

- Existing Statewide Communications Interoperability Plans (SCIP) and Tactical Interoperability Communications Plans (TICP)
- Existing strategic plans, both business and technology, establishing requirements that agencies must meet
- Debriefings and after-action reports on incidents, particularly multiagency incidents
- Evaluations of table-top and full-scale exercises
- National Emergency Communications Plan (NECP) goal performance national reports

Make written or mental notes of needs and requirements apparent in these sources that otherwise may not surface during interviews or focus groups. Use them to elicit discussion, perhaps validating or tempering issues raised.

☐ Be Prepared: Collect Scenarios

Emergency response scenarios used in planning, training, and exercises provide a ready-made source of examples that can be presented during interviews and focus group sessions. With any luck, agencies involved in your project already regularly conduct multijurisdictional exercises. Those scenarios can be tapped. Emergency management officials can provide other suitable strategies.

Other good sources include the SAFECOM *Public Safety Statement of Requirements*[37] and the Department of Homeland Security's National Planning Scenarios. Both are rich sources of examples of everything from natural disasters to improvised nuclear devices. Check with your local or state emergency management offices for details of the National Planning Scenarios.

A ready supply of scenarios provides fertile ground for eliciting needs while talking with stakeholders.

☐ Conduct Interviews and Focus Groups

Once prepared with background, you're ready for direct interviews and focus group sessions with stakeholders to uncover needs related to project goals. Interview and facilitation skills can be learned, but they require practice. If this is your first project, you're definitely jumping in feet first!

Interagency projects generally bring more stakeholders, many of whom should be interviewed or involved in focus groups for collecting needs. Whether this is your first project or you're a veteran, read Chapter 5 of the original *Law Enforcement Tech Guide*. It provides a wealth of information on interview and focus group techniques. You're bound to pick up a few pointers!

37. U.S. Department of Homeland Security, SAFECOM Program, *Statement of Requirements for Communications and Interoperability*, Washington, D.C.: Volume I, Version 1.2, October, 2006. See www.safecomprogram.gov/library/Lists/Library/Attachments/302/Statement_of_Requirements_Volume_I%20-%20Version%201_2.pdf; and U.S. Department of Homeland Security, SAFECOM Program, *Public Safety Statement of Requirements for Communications and Interoperability*, Washington, D.C.: Volume II, Version 1.2, August 2008, See www.safecomprogram.gov/library/Lists/Library/Attachments/302/Statement_of_Requirements_Volume_II%20-%20Version%201_2.pdf.

☐ The Product

By the completion of the interviews, the needs analysis process will have produced an abundance of information. This Guide has concentrated heavily on data collection so far; next, we'll turn to distilling all that has been collected into general system requirements to be included in design documents.

Needs Analysis 103: Develop General System Requirements

Business process baseline development, stakeholder interviews, and focus groups yield three kinds of needs: Organizational, Operational, and Technical. Each will develop into requirements separately. Some will naturally be used for procuring technology to improve interoperability; others will be acted upon by the agencies themselves, individually or collectively.

> Life was simple before World War II. After that, we had systems.
> —*Admiral Grace Hopper*

For a complex system of interoperable systems, requirements will span agencies, response disciplines, modes of service delivery, and communications systems. They rightfully describe everything from training and proficiency of users to availability and reliability of system functions, such as radio coverage, or standards-based development of RMS information exchanges.

These requirements are used in a conceptual design that incorporates action plans for organizational and operational change, as well as in technology procurement and implementation documents. The iterative process of collecting baseline (as-is) information, assembling needs across stakeholders, and generating system requirements (to-be) necessitates repeated participation, review, and comment by working committees—both operational and technical.

Describing Requirements

Understanding and articulating your requirements is key not only to any successful procurement of technology, but also to organizational and operational changes necessary for improved interoperability. Requirements have to be described in terms directly linked to the interagency business processes to be supported. Operational requirements are best stated in simple terms, avoiding constraining definitions of how requirements will be met.

Describe requirements using consistent terms and categories that help make sense of what otherwise might be a confusing jumble of data. Fortunately, common terminology and basic categories have evolved. SAFECOM's *Public Safety Statement of Requirements* provides some of the most useful standardized descriptions specifying with whom, for what purpose, and under which special conditions a series of typical communications may occur. While looking toward future development of technologies, the documents use a complete and consistent style of description. We've used elements in business process examples above that would roll into requirements documents.

Communications requirements can be described from several different angles. We can look at the type of communications, the technological modes traditionally used to provide them, and the operational modes of response when they're used. We can also describe them in terms of their scope, scale, and priority.

Use the categories and terminology in Figure 6-2 in stating requirements. Quantification and qualification are both appropriate.

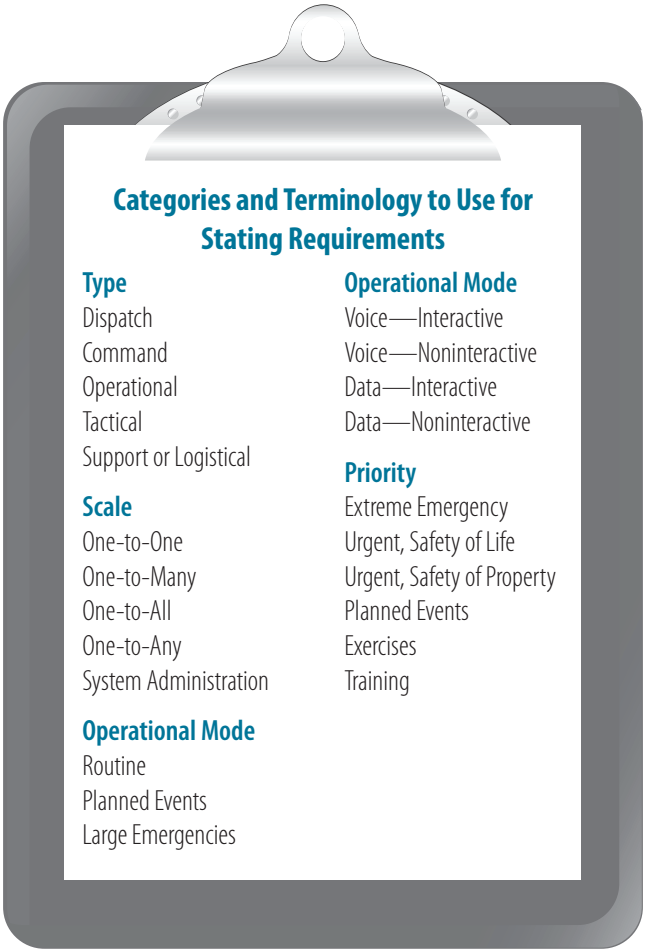
These methods of describing communications—either as they currently are or as they should be—serve to categorize them. Categorization is useful for understanding different requirements and being able to explain them. This is necessary not just for specifications when buying communications systems, but more important, for understanding internally what we're doing with communications. Simply adopting common terms to describe communications goes a long way in communicating—no pun intended—what's going on when writing standard operating procedures, training, conducting exercises, and working with other agencies to improve interoperability.

Note that these ways of describing communications aren't mutually exclusive and, in fact, definitions are bound to vary across jurisdictions and disciplines.

Step 1
Define General Functional Requirements

Requirements are next defined in functional terms and compiled into a report presenting them along with a conceptual design that illustrates how they fit together. The first step in pulling together that report is to compile requirements from preceding work. Functional requirements are defined in terms of just how the "system of systems" will work to accomplish your project's goals and meet its vision.

Figure 6-2: Categories and Terminology



Don't allow preconceived "solutions" to slip into your requirements. The price to pay in noncompetitive bids that are challenged is just too high—and you may not get the best solution for your operational needs. The project manager bears the responsibility for identifying conclusions that may have slipped in under the guise of requirements.

Sort requirements into organizational, operational, and technical categories.

☐ Organizational

Interoperability needs analysis generally produces a number of requirements for organizational change or development. Some examples include needs to create the following: memoranda of understanding for sharing costs, mutual aid agreements for sharing resources, policies for incident management during multijurisdictional emergencies, and procedures for interagency operations. Requirements may also include standard practices for life cycle funding of systems, minimum staffing of deployable communications resources, security, and standard training on interagency communications across all partners.

The project's executive sponsors and Steering Committee bear the responsibility for preparing their organizations for changes necessary to improve interoperability. Most organizational requirements that arise will require changes only possible through their leadership.

Give some thought to what has been documented through the process up to this point. Separate those requirements that have been expressed that can best be addressed by management. They'll be used in the conceptual design.

☐ Operational

Collect the processes and needs that have been expressed in operational terms. If you followed our advice in completing the business process baseline, you're well on your way. Additional operational requirements arising from interviews and focus groups must be folded in, but they should be obvious if you focused on operational outcomes of interoperability.

Beware of operational needs that extend the scope of your project. The primary reason for establishing scope early in the project under the direction of the Steering Committee is to draw some boundaries around what specifically is to be accomplished. Hopefully, you were able to use the project scope to keep the needs analysis focused, but in case some discussions veered off-track, now is the time to start paring back.

Remember: it's all about inter-*operability*. Operational outcomes are the whole reason why your project was undertaken. Take the business process descriptions and needs that have been developed and massage them into statements of requirements that describe how the pieces must function together.

A good technique is to use scenarios that you collected to facilitate stakeholder interviews and focus groups to describe operational requirements, highlight technology already in place, and state technical constraints. Realistic examples always serve to clarify.

☐ Technical

Technical aspects of functional requirements address how operational needs are to be met through technology. Don't confuse them with the technical details of existing systems that went into the baseline reports and will go into requirements for interfacing or integrating those systems with any new technology. Because few agencies maintain communications engineering staff, consultants are often hired in communications projects to examine the technical environment, document technical requirements, and then define interface and integration requirements described in the next step.

Communications technical requirements are often expressed as a matter of one or more qualities, such as:

- Capability – services provided for emergency responders (what, who)
- Availability – how well the system covers the area served (where)
- Reliability – how well the system delivers its services (when)
- Scalability – how well the system accommodates surge conditions
- Survivability – how resistant the system is to failure
- Restorability – how easily the system is restored upon failure

The Technical Committee may not have defined its needs using these terms, but we're certain the terms were touched on in principle. Use these qualities to further categorize technical requirements. State them in ways that can be tested and validated by system users.

Use terms of quality to state technical requirements.

Avoid requirements that are essentially technical specifications. When system vendors deliver technology according to technical specifications and it doesn't meet operational needs, the technology or vendor is usually faulted. In reality, the failure was in not stating requirements so that operational tests could prove whether the solution was acceptable.

While a simple idea, stating requirements in functional terms takes work. It's tempting to adopt specifications as requirements, and then be forced into using technical performance measures for acceptance. Within your project, work to assure you understand operational requirements well enough to decide whether any proposed solution—technological or otherwise—meets needs.

Regulatory mandates often spur system upgrades and replacements.

The Technical Committee may have expressed needs to meet federal and other regulatory mandates. For example, the Federal Communications Commission (FCC) released rules regarding rebanding (moving existing channels within a band to reduce interference)[38] and narrowbanding (reducing the amount of radio spectrum used for a given channel).[39] The committee may also have identified limited radio spectrum as constraining expansion of systems to meet other needs.

These types of mandates provide the primary impetus for many communications system upgrades and replacements. Note that, properly speaking, they don't represent requirements for your interoperable systems, but rather are part of the environment in which realistic solutions have to be implemented. For example, there is a difference between a requirement to meet FCC narrowbanding regulations and a conclusion to migrate systems to the 800 MHz frequency band. While that might be the eventual solution, there's a difference between making it a possibility and making it a requirement.

Step 2
Define General Interface and Integration Requirements

All systems have geographic, functional, and technical boundaries that have to be bridged and every interoperability project has internal points of interface between communications systems and subsystems. Very few projects are initiated to uproot all communications components for all agencies—from voice radios, to backbone networks, to consoles and beyond—so integration of the old with the new is generally inevitable.

Your own project probably encompasses components that won't be replaced in this effort to improve interagency communications. Ideally, they can all be integrated to the extent they can honestly be called a "system of systems."

38. In August 2004, the FCC initiated the process of relocating most public safety 800 MHz users within the band to reduce interference suffered from commercial wireless systems.

39. In December 2004, the FCC released long-awaited rules that will force eventual changes to all radio systems operating below 512 MHz—all the commonly-used public safety bands below 700 and 800 MHz. By January 1, 2013, all radio channels used by these systems must be reduced in width by half or be capable of passing at least two voice conversations in the same amount of radio spectrum.

This step in defining requirements establishes what parts of existing systems will stay and which may go. It defines required points of interface between those that stay and any new technology that may be implemented. This is the place to document specifications that will shape proposed technology solutions.

Start by describing the core systems and subsystems that exist and will be built upon. Establish provisional requirements for using them in concert with any new interagency communications capabilities. The person responsible for managing the agency's technology and information systems may have information that will help streamline this task. Part of managing information technology (IT) systems is to keep track of configuration items (IT components and services) and document their versions, status, and relationships with other systems.[40] It is common for agencies without dedicated IT staff to lack this information. If you outsource your support and maintenance, your vendors should have what you need concerning their components. As you gather the information on these items for your project, take the opportunity and commit to maintaining the records. Future systems will be more reliable, more efficient, and cost less as a result.

For example, consider the popular gateway devices that connect audio between different radio systems, effectively patching two or more channels together. In some areas of the country, these are critical resources for enabling interagency communications. Many have been placed in fixed locations and have limited capacity for expansion, either because of some inherent limitation on the number of channels that can be interconnected or because the radio site is otherwise congested. Requirements for connecting the gateway into any new means of interagency communications should be spelled out.

Or consider that advanced radio systems are connected by sophisticated backbone networks carrying all sorts of voice, data, and other forms of communications. Quietly in the background, the network is probably carrying supervisory control and data acquisition (SCADA) information that's used to manage the network itself, radio sites it interconnects, and maybe even radio tower lights! (Don't laugh. The cost of burned-out tower lights can be high—federal fines and worse!) Any new systems added to such a backbone may be required to interface with the SCADA subsystem.

Now is the time to establish any requirements on integrating other systems through these and other resources. By nature, interface and integration requirements are very technical. Internal or contract engineering expertise can be put to work in defining these requirements.

40. Foundations of IT Service Management, based on ITIL V3; ITSMF International, 2007.

Step 3
Create a Conceptual Design

This is your *to-be* report.

The final step in developing general system requirements is production of a conceptual design. This document illustrates how interoperability goals are to be realized through both technical and nontechnical means. It demonstrates a vision incorporating major assumptions and constraints, highlighting functional outcomes of your project.

Create the conceptual design from the requirements statements you've assembled. While much of the document will be essentially a narrative of what your needs analysis produced, don't forsake the pictures! Maps and diagrams are particularly important components to include because they capture a great deal of information in one place and show relationships difficult to explain without a lot of verbiage. Use sequence and flow work models from the business process baseline assessment to illustrate what exactly will be supported by any new systems to be implemented.

Once again, the project manager is responsible for this product, but don't feel bad if the whole needs analysis process has left you exhausted! It's not uncommon for it to be contracted out. System integrators strong on business process reengineering and less interested in communications systems engineering have done some of the best work we've seen in this regard.

As mentioned, this is a conceptual design for improved interoperability that most likely will require a lot of organizational development, as well as technology. Don't confuse it with more detailed engineering designs that will come with responses to any significant request for proposals and technology implementation plans. Those come later—if at all—and address technical aspects of interoperability solutions.

Needs Analysis 104: Evaluate *Buy* Versus *Build* Options

We've come to a decision point: What share, if any, of your new interoperable system of systems do you want to own and what share are you willing to outsource?

Don't buy the house; buy the neighborhood.
— *Russian proverb*

This is a difficult decision that must be made before procuring any services. Traditionally, public safety agencies have built, owned, and operated their own communications systems. Whether for voice or data purposes, police, fire, and EMS agencies have traditionally chosen to "rule their own" systems to provide known levels of security and services, manage long-term costs, and guarantee priority access during emergencies. However, agencies increasingly use commercial services for data and even some voice traffic.

Public safety agencies have traditionally ruled their own radio systems.

Voice push-to-talk communications is considered the most sacred technology owned and operated by public safety agencies. While very few agencies have resorted to completely outsourcing radio needs, every day more and more move traffic off traditional voice radio channels and onto data systems, cellular telephone, and other commercial radio services. Hybrid systems, owned and operated by private companies but leased to public safety, are also increasingly common.

Commercial networks are increasingly used in mobile data systems.

Some share of this migration is due to the lack of available radio spectrum for new and growing uses, but the trend is also seen in areas where frequencies aren't so scarce. We expect this trend to be cyclical as the costs of building, operating, and maintaining systems is weighed against the costs of sharing access, opaque commercial capabilities that can't be examined in detail, and less control over services received.

Shared systems bring high levels of technological compatibility.

An important choice about joining shared radio systems may also be in your cards. These regional or statewide systems are being built to take advantage of economies of scale, gain strength through numbers with vendors, make use of otherwise duplicated system components, and improve technological compatibility that can lead to better interoperability. In many ways, they offer a good compromise between buying and building new radio systems. Connecting with your Statewide Interoperability Coordinator (SWIC) and reviewing your state's SCIP is a good place to start if you are interested in learning about opportunities to leverage your resources in this way.

If the option is available, use of a shared system may be a partial or possibly a complete solution to your project's technology needs. This may result in similar deliberations about guaranteed levels of service, long-term costs, and priority access that you would have when using commercial systems. Approach participation in shared systems in a manner similar to procuring a new system or commercial services, recognizing the "added partners" you get at no additional cost!

This completes your needs analysis. The products will have been presented in large part to stakeholders and accepted as formal project documents. Now is the time to complete a project plan.

CHAPTER 7

Scope the Work To Be Done

What: A scoping exercise examines the extent of organizational and technological work to be done through procurement and implementation. It concludes with the decision of what work to contract out and what to complete in-house.

Why: Communications projects include work that you may wish to undertake directly or contract out. Understanding the work involved allows a choice of what will be included in the procurement process and who will be responsible for different aspects of the system.

Who: The project manager needs to understand both the work to be done and internal resources available to complete it. The Steering Committee ultimately has to decide what will be done internally and what will be procured externally.

When: Following the needs analysis, the work to be done should be examined and decisions made on what services and equipment will be procured.

We left the needs analysis phase of your project with a conceptual design in hand and a "buy or build" decision on how to improve communications interoperability. The conceptual design described at a high level how the various system components—technological and otherwise—will fit together for interagency operations. In preparing a project plan, look at the scope of work to be accomplished and decide who will accomplish what (refer to Chapter 8: **Create a Project Plan**, Step 1, **Draft a Scope Statement**).

The remaining phases of your project are procurement, implementation, and maintaining the systems and processes. Each project phase requires a good deal of work from the project team, but you will soon be at the crossroads of deciding what to hand over to contractors and what to do internally.

In order to best make that decision, it's useful to understand what has to be accomplished, particularly tasks that are most commonly contracted out.

Commonly Contracted Services

Radio and other communications systems involve a number of specialized services. Those discussed below are broad categories of work commonly contracted out—either separately or together.

Project Management

Obviously, there has been—and remains—plenty of project management work yet to be done. This whole book *and* the original *Law Enforcement Tech Guide* are dedicated to helping with that work. Project management will probably seem like more and more work as you read along!

Keeping with prior assumptions, we'll continue to assume you are reading this as the designated or soon-to-be project manager. In moving toward system implementation, you have to work ahead to create a project plan, develop teams, carry out procurement, lead contract negotiations, and build an implementation plan. You'll need help, but we'll assume the job of project management will be held pretty close to home.

System Design

Do you need further system design at this point?

You may already be facing a conundrum that many others developing complex systems have grappled with: do you need further system design before proceeding to procurement?

Many projects proceed to procurement with little more than a conceptual design, functional specifications, and some boilerplate language. This is done to leave the field open for innovative vendor proposals. Other projects proceed through an engineering design that yields very detailed specifications for bid.

Don't limit your choices by over-designing technical elements.

For interoperability projects, our recommendation tends more toward the former approach than the latter. Interoperability projects involve many existing systems and complex needs that may best be addressed by technologies you haven't anticipated, so it's best to remain flexible.

Alternately, you may choose to hire a system designer before embarking on a general system procurement process. This may become a more common process for interoperability projects as funding becomes predictable, but now it is used more often for complete, new radio systems.

Detailed Engineering Design

Complex systems require a detailed engineering design that is very dependent on the technology chosen. For this reason, the most detailed designs are usually left as an early deliverable for the contracted system vendor.

System Installation and Optimization

Commonly done by the primary equipment or system vendor, the task of systems installation and optimization occurs during implementation. Projects without a predominant vendor or those employing multiple technologies may require independent contractors. Each may install and optimize different parts of the system, such as its voice radio infrastructure and its microwave backbone. In this situation, your project could require system integration services.

System Integration

The role of a systems integrator is to take the variety of electrical, electronic, and physical system components and (surprise!) integrate them into a coherent whole. Integrators often also serve in system design, acceptance testing, and quality assurance roles.

This is a role you may choose to handle with project staff, contract independently, or leave up to a system vendor as a turnkey procurement. A *turnkey procurement* is one in which a general system vendor or equipment manufacturer serves as the system designer, integrator, and equipment provider.

Turnkey procurement: One in which a general system vendor or equipment manufacturer designs and integrates the system, and provides the equipment.

We'll provide recommendations on how to proceed with these particular choices near the end of this chapter.

Quality Assurance

Often used to refer to a broad range of acceptance testing (see page 120), *quality assurance* is defined as a systematic process for assuring that a project meets its objectives. Quality management is formally part of project management and is most commonly seen in large system implementations.

Independent quality assurance contractors are occasionally used for radio projects. For example, the Illinois State Police hired a quality assurance consultant to evaluate proposals for a statewide system for the State Police and other state and local agencies.

Acceptance Testing

Acceptance testing is dealt with in more detail in Chapter 10, **Implement the System**.

In implementing technology, acceptance tests are planned and conducted to determine whether specifications and performance requirements are being met. The larger the project, the greater the effort involved in acceptance testing. Complex measures of performance, such as radio coverage, may be included in the acceptance process.

While it's always valuable for the customer to be involved in acceptance testing, part or all of the effort is occasionally contracted out to an independent party due to the work involved.

Other Work to Be Done

There are three additional areas of work involved in implementing communications systems where agencies typically choose to retain greater control: training, radio site development, and frequency licensing. Each of these areas can be completely outsourced, of course. However, it's more likely that you would keep a tighter rein on them than you would, for example, on microwave path analysis.

Let's take a look at each of the areas in some depth to provide more background for your choices in delegating or contracting project work.

Training

Training is the key to your successful system of systems.

Training will be the key to your successful system of systems. Anticipate that several types and levels of training will be necessary. Consider what may best be done in-house, and what can be contracted from your system vendors, or even solicited independently from training companies and organizations.

☐ Technical Training

Your equipment vendors can be expected (under contract!) to provide training on the technical operation and maintenance of equipment. Depending on the type of communications project, this training is appropriately provided to agency radio or information system technicians. Ongoing training should also be anticipated for new staff members and to maintain the skills of existing ones.

☐ Dispatch User Training

Many means of improving communications interoperability will rely on that central resource for most emergency response: the public safety telecommunicator or dispatcher. Comprehensive dispatch user training is essential. The dispatcher's role requires their own personal integration of so many communications systems that you shouldn't underestimate the need for carefully designed and executed dispatcher training.

Dispatchers are professional systems integrators.

☐ Field User Training

Last, but not least, field responders who will use the system to communicate across agencies and jurisdictions need training. For all agencies planning to use the system, develop a comprehensive program that provides initial training of existing staff, basic training of new staff, and coordinated interagency exercises. Consider that such training won't appropriately come from system vendors, but from your own agencies' staff or even specially contracted assistance.

No technology is so simple that training is unnecessary for people who will use it during emergencies.

Radio Site Development

One technical consideration that agencies often maintain some control over is the selection of radio sites for systems. Vendors rarely know as much as your users do about how well sites serve current needs. There's a good deal of "give and take" between project technical committees and vendors in the process of radio site selection for new and expanding systems.

If you anticipate much radio site development in your project, make sure to include people on the Technical Committee who have the knowledge and background of what's currently in use. There's usually a lot of history behind why a particular site is used and why a better one is unavailable. This sort of "corporate knowledge" is the type that you don't want to pay a contractor or consultant to rediscover.

Include staff on the Technical Committee who know what's in use—and why.

Basically, radio sites are real estate. The three most important aspects of their selection are location, location, and location (we're sure you've heard this before about residential real estate!). If your project requires site work or development, you're faced with using current system sites as-is or with improving, buying, or leasing access to other existing sites, or developing entirely new ones. In all situations it is important to keep an eye toward the future; what looks like a good location today may not work a few years from now.

The overriding consideration for sites is the coverage they will provide.

The overriding consideration for radio sites is the coverage they will provide. This is affected by physical location relative to the involved jurisdictions, height relative to the area to be covered, surrounding natural or man-made clutter that will block radio waves, and other electromagnetic factors. While there are always compromises to be made, ***coverage is king***.

Considerations for existing and new sites differ a bit.

☐ Considerations for Existing Radio Sites

DHS considers public safety radio sites, and communications and information sharing systems, as critical infrastructure. The National Infrastructure Projection Plan (NIPP) provides information on strategies to protect these systems. For more on the NIPP, see www.dhs.gov/files/programs/editorial_0827.shtm.

- **Physical access.** Is the site constructed for safe, secured access for all tenants? How does the site manager provide for installation of new equipment on towers and in shelter space? Is there a security system to keep out unwanted visitors, yet not impede legitimate maintenance?
- **Physical space.** Is there "prime" tower space available for antenna systems? Does the shelter rack have expected space for radios and antenna system combining equipment?
- **Services.** Is commercial and backup power suitably sized for all users? Is an adequate lightning protection system in place? Do the electrical and radio frequency (RF) grounding systems meet electrical codes and industry standards?
- **Maintenance and monitoring.** Is the site well maintained to minimize the tenants' costs and reduce their liabilities? Does it have an adequate monitoring system for tower lighting, power systems, and security controls? Has the site manager instituted an acceptable plan for minimizing exposure to incidental electromagnetic radiation, as required by the FCC?

Federal Aviation Administration (FAA) permits often require tower lighting. Not only are tower owners liable for lighting inadequacies or failures, but tenants' leasing space have been fined, as well.

- **Electromagnetic compatibility.** Are there other users of the site whose systems will make it impossible or expensive for your systems to work? Is there a powerful radio paging service operated nearby that may interfere?

☐ Considerations for New Radio Sites

For the uninitiated, building a new radio site is an education. Many an initiate has begun the process to develop a seemingly crucial location and ended up regretting getting started in the first place! While not impossible to do and do well, of course, new site development requires a lot of work that you may have not anticipated. Consider all that is involved before insisting on doing it yourself.

Here are some initial questions regarding a system design involving new sites:

- **Property ownership.** Do project partners already have suitable locations for new radio sites or access to other publicly-owned property? Is there potential private property that can be purchased or leased?
- **Physical access.** Are good roads available nearby for construction and maintenance of standalone sites? Is facility access adequate for those being put up on buildings, water towers, and other existing structures? Is there an adequate road right-of-way to the property? Is it accessible throughout the year or will seasonal conditions affect needed maintenance?
- **Physical space.** Is there sufficient space available to put up a tower and equipment shelter? Is there sufficient space for back-up power generation?
- **Security.** Can the site be adequately secured from vandalism and unauthorized access? What level of access control is possible? Can systems be monitored for damage or failure?
- **Utilities access.** Are commercial power and telecommunications available or economically accessible?
- **Existing backbone networks access.** Will connections to other backbone networks owned by the agencies be practical from the site?

Be aware of grant limitations on purchasing sites or permanent construction! Many won't cover it outright, but will accept the costs as an allowable match.

Some additional considerations in implementing radio systems with new sites are:

Buying or leasing real estate. For government agencies, this inevitably requires a lot of legal and financial consideration by staff elsewhere in the affected jurisdictions. If you hadn't included suitable expertise in an ad hoc working group, you will want to add it if you plan to acquire new site real estate.

One jurisdiction had to resort to condemning private property for right-of-way access to an important radio site.

Zoning and variances. You may run into zoning issues for a given location that require navigating the thorny path of property use variances. Even if a formal variance is unneeded, plan on a careful, measured public hearing and education process if you plan to put up a new tower. There's a wide and strong current of NIMBY ("Not in my backyard") running nationwide. Not everyone sees the beauty in radio towers and there's always concern about the potential health effects of nearby radio transmitters. Plan to use a public relations team to help you if you choose to get into the business of building new radio sites.

One jurisdiction ran head-first into a "Save Our Mountain" committee when trying to site a new tower. They ended up compromising on the location—going with a marginal bench on the side of the mountain rather than on the top to avoid tower lighting requirements—and ended up suffering coverage problems in critical areas for more than 20 years.

Construction permits. It should come as no surprise that all the work going into a new site generally requires studious attention to obtaining building permits. As public agencies are often under great scrutiny, your partners will expect that all necessary and appropriate permissions are received before construction begins. This needn't be a difficult process, but it does take time and often affects site design.

Increasing use of "mesh" radio networks for data requires many more sites, though generally simpler ones.

Tower size. A tower's height above ground or above the average terrain surrounding a site dramatically affects the coverage of radios in all frequency bands. While there are technical design trade-offs—too much height, too much coverage, the effects of distant interference aggravated by being in "too good" of a location, and general practical construction considerations—greater height for antennas is generally preferred to maximize the coverage.

Building new sites brings up additional engineering considerations before real estate is ever purchased. Tall towers require guy wires that run to ground anchors well away from the towers, necessitating larger sites and additional construction, including security fencing. In 2004, a Florida jurisdiction suffered a dramatic and dangerous tower collapse when a service truck backed into guy wires at one of its sites. Such total loss of a site can have a dramatic effect on system capabilities.

FAA permits. Radio towers and antennas can be serious aviation hazards. The FAA has strict regulations regarding their location, size, painting, and lighting. Don't plan on putting up new towers without scheduling time for the FAA permitting process. Antennas or mounting structures that don't extend more than 20 feet above existing structures don't require additional approval, but when it is necessary, plan on 6 to 8 weeks for completion of permitting.

Environmental and cultural assessments. A common "gotcha" in building new radio sites is the need to conduct assessments of the environmental impacts of new sites. Many potential sites are in environmentally sensitive areas and may be subject to the National Environmental Policy Act (NEPA). Environmental impact statements are

time-consuming and can bring public contention. Similarly, potential sites may have historical or other cultural significance that can quickly exclude their consideration or require careful assessment.

Rely on expertise in your jurisdictions' building, construction, and zoning divisions, as well as legal staff, to help decide whether environmental and cultural assessments will be necessary for new sites. Be aware that there are private companies that specialize in doing this work, as well.

☐ Other Radio Site Work

If you choose to be involved in the selection of any radio sites to be used in your new system, be aware of the additional work this typically involves.

Site inspections are important and typically required by vendors when existing sites will be used for new or extended systems. Inspections may be conducted by a joint team of your project's technical members and the vendors, or it may be stipulated in contracts as being done by a third party. Commonly, vendors look for adherence to commercial or public safety standards before accepting sites offered by agencies for use. Conversely, you may have nontechnical requirements for sites identified by vendors, such as access for maintenance and physical security.

Vendors look for adherence to commercial and public safety standards in evaluating existing sites.

Tower inspection and validation is related to site inspection, but considered a separate task because of the engineering expertise needed to evaluate the structural integrity of towers and validate their acceptability within the engineering design.[41]

Site design is a separate, but important task. For new construction, it starts with layout of the tower, shelter, guy wires, grounding systems, utilities, access, and security. For new or existing sites, floor plans have to be developed and documented to assure adequate space for equipment and its proper identification later on. Similarly, equipment rack layouts are an important part of site design. Radio sites are dependent on adequate, quality electrical service that typically has to be converted from the utility company's alternating current (AC) to direct current (DC). An electrical design is needed that accounts for AC service to some pieces of equipment, DC to others, and backup power when commercial service is lost. Proper documentation of all these site design elements is a critical deliverable during implementation, too.

For new or existing sites, adequate floor space has to be available for expected equipment.

41. The National Association of Tower Erectors (NATE) works with federal agencies and standards organizations to establish tower safety practices. See www.natehome.com.

Antenna system installations are generally part of any implementation of new fixed radio infrastructure. More than likely, this responsibility will be defined in your procurement documents as either your responsibility or the vendor's. In either event, both parties have an interest in using certified crews for the sake of safety and quality.[42] If you require the vendor to use existing antenna systems or ones your agencies provide, expect the vendor to require their own verification of suitability.

Frequency Coordination and Licensing

Most public safety transmitters have to be licensed with the FCC.

The final area we want to address in scoping work to be done is licensing of any required radio frequencies. Not all projects will require additional channels, but licensing is generally required for any addition of new sites, even on existing frequencies. Don't make the mistake of planning to put in new transmitters of any form without assessing FCC licensing requirements.

Spectrum congestion forces agencies to move to new frequency bands to get new capabilities.

There are a multitude of considerations about RF spectrum availability. It's beyond the scope of this Guide, but suffice it to say there are very definite limitations in most areas of the country, using predominant frequency bands, in adding new frequencies to systems for interagency use. Since compatibility with existing systems and surrounding partners is a central issue in communications interoperability, there is rarely the ability to uproot all systems and move to new, typically higher, frequency bands to find "green space."[43] Projects of the type we're addressing in this Guide are more incremental in nature, typically not requiring large numbers of new frequencies.

Whether new frequencies will be required or existing ones used in new ways, the FCC requires frequency coordination and licensing. The application process itself is alien to most agencies and uncomfortable even for most technicians. Many agencies have technical staff adept at preparing applications and navigating the frequency coordination process. Both activities have become more complex in recent years, however, and agencies are increasingly outsourcing the whole process of systems acquisitions.

42. The Occupational Safety and Health Administration (OSHA) and National Institute for Occupational Safety and Health (NIOSH) have increasingly stringent standards affecting tower construction and antenna system installations. See NIOSH Publication No. 2001-156, www.cdc.gov/niosh/docs/2001-156/.

43. SAFECOM produced a publication addressing the subject, *Public Safety Radio Spectrum: A Vital Resource for Saving Lives and Protecting Property.* See www.safecomprogram.gov/library/Lists/Library/Attachments/211/Public_Safety_Radio_Spectrum%20-%20A_Vital_Resource_for_Saving_Lives_and_Protecting_Property.pdf.

For purposes of planning, be aware that the cost of license application preparation can range from a couple hundred dollars to several thousand for larger, more complex systems. The FCC doesn't charge fees for licensing by public safety agencies of their land mobile radio systems,[44] so no cost is to be anticipated there. It does, however, allow certified *frequency coordinators* to charge for their services.

A couple of certified coordinators use local advisors, people within the state or region who typically work in a technical capacity for a public safety agency that volunteers their time.

Frequency coordination is the process of selecting appropriate frequencies for the applicant agency, while balancing the needs of other eligible users and minimizing interference between all.[45] Since practically all licensing that public safety agencies do requires frequency coordination, you can anticipate using the services of a certified coordinator. The FCC maintains a list of coordinators and contact information on their website.[46]

We increasingly see projects where certified frequency coordinators are brought on under contract to help guide this aspect of design, and then subsequently prepare applications, coordinate frequencies, and submit everything to the FCC. Fees are typically based on the number of frequencies and sites used in a system. Again, the cost varies according to the size and complexity of the system. It varies from a couple hundred dollars for a simple modification to an existing license to tens of thousands of dollars for new systems with many sites and frequencies. For planning purposes, contact the certified frequency coordinators for cost estimates.

GATEWAYS AND FREQUENCY LICENSING

Gateways that interconnect multiple radio systems bring additional licensing requirements when used to directly control transmitters. Requirements vary based on whether the device is used to connect fixed radios or is displayed as a mobile device.

Check with the FCC-certified frequency coordinators on what additional licensing will be required for transmitters connected to your gateway. Don't forget to include potential federal partners in formalized agreements. For more information on formalized agreements like Memorandums of Understandings, see Chapter 11.

44. *Land mobile radio* (LMR) is a particular classification of radio systems that includes common dispatch, car-to-car, and portable communications used by public safety agencies. License fees are required for other types of wireless systems, such as microwave links.

45. The Association of Public-Safety Communications Officials – International, Inc. provides an explanation of frequency coordination on its website. See www.apco911.org/frequency/.

46. See http://wireless.fcc.gov/publicsafety/coord.html.

Assessing the Scope of Work to Be Done

You have reached a decision point. Just how big *is* the project and how much of it do *you* want to take on? That might seem like a philosophical question (particularly if you were, well, *assigned* to manage the project), but from a more practical and less personal standpoint, here's a consideration: do your agencies want to have the fine-grained control over all system acquisition and implementation activities that yields the most customized and highest performance system, or are you comfortable handing off some or all of that responsibility for manageability?

What are the Choices?

Don't rely on vendors' measures of "interoperability."

It's not an easy decision and not necessarily black and white. At one end of the scale are agencies that have relied on a single vendor for so long that they will buy whatever the vendor offers as an "interoperability solution." Not only will they buy it, but they'll use the vendor's functional and performance specifications to evaluate "success." This is an abrogation of responsibility that leaves real needs unsatisfied.

Consulting for major systems design and implementation can be expensive because there's a lot of work involved.

At the other end of the scale, some agencies proceed with large systems design and acquisition by being the general contractor, so to speak, themselves. They take on all responsibility for engineering design, construction, acceptance testing, and integration of the diverse subsystems that make up modern communications systems. What they can't do in-house, they contract out piece by piece. The advantage is better needs-based design and project accountability. The disadvantage is that it can be a huge amount of work.

In between these extremes is the rest of the world. Few agencies have the internal resources to take on all these duties, so usually end up contracting out some or all of the tasks that have to be accomplished in a big system implementation. The trade-off is in finding the right contractors to take them on. And, of course, every project is going to have a different combination of the required tasks.

What Will You Handle Internally?

How do you decide what share to handle internally? Start by looking at the participants' willingness to define the scope and level of work required. By this point in your project, you should have a pretty good idea of internal resources available for the work ahead.

Of course, major system vendors are very willing and usually quite interested in taking care of all your needs. While this comes at a cost, don't forget there is a good reason for this: vendors will undertake tasks that you may not have adequate or appropriate resources to do. As you proceed, consider which roles are best managed closely for your project and with your resources.

Recommendations

Our recommendations on proceeding through procurement to implementation are based on the scope of the project as reflected in its anticipated cost.

For systems expected to cost less than $500,000, plan to act as your own general contractor. Rely on either internal engineering expertise or contract for it. Little site development is expected for projects this size, so engineering is reduced. For projects of this size and smaller, agencies often rely on regional service companies with whom they have existing contracts.

Independent integrators can be more objective in advising you of needed organizational, operational, and management changes.

For systems up to a few million dollars, consider using a turnkey procurement where the winning vendor will take care of all the system design and implementation work. Projects of this size are generally larger than what agencies can comfortably take on themselves and small enough to make contracting for the parts separately unnecessarily time-consuming and costly. A project management or quality assurance consultant may be a good investment to improve your project's odds of success.

Our recommendation for systems costing more than a few million dollars is to hire a systems integrator separate from the primary technology vendor or vendors. This gives you more direct management control of the project. Good integrators can help not only in moving your project from conceptual design through implementation and on to full operations, but also by bringing a wealth of experience in dealing with technology vendors. Their reputations are built on assuring project quality for their customer—your agencies—by getting the most for your dollars.

Develop Your Own Recommendations and Get Approval

These recommendations are just rules of thumb, of course. You and your project team are the best judges of what can reasonably be accomplished internally and what can affordably be outsourced.

With the consensus of the User and Technical Committees, seek Steering Committee approval to move forward with further project planning and procurement based on the agreed-upon scope of work. With this approval in hand, you're ready to create the project plan!

CHAPTER 8

Create a Project Plan

What: The project plan is a document that guides the entire design, procurement, implementation, and future operation of an interoperable system. It provides the detail necessary to manage each phase of the project and the multitude of activities involved in each. It includes components for controlling the critical Scope-Budget-Timeline relationship,[47] as well as managing risks and communicating about the project with stakeholders. This document will evolve over the life of your project.

Why: Project planning—the dynamic process of creating a project plan—dramatically increases the chances for success of interoperability projects. Plans keep both internal and external stakeholders informed in varying levels of detail. They provide the means to control activities, detect problems early on, and respond to changes along the way.

Who: The project manager and the User and Technical Committees are involved in discussions, decisions, and research. The project manager should be responsible for project plan documentation. The Steering Committee and executive sponsor must endorse and sign the plan.

When: Creating a project plan should follow the formal development of the decision-making structure (Chapter 5) and in conjunction with the development of the needs analysis (Chapter 6).

Project planning is the focus of Part 3 of the original *Law Enforcement Tech Guide*. The topics of scope, timelines, budgets, risk management, and project communications are dealt with in depth through its six chapters. This chapter draws heavily from them, while emphasizing key aspects for interoperability projects.

Chapters 8–13 of the original *Law Enforcement Tech Guide* deal with project planning for technology projects in general.

47. As mentioned in the original *Tech Guide*, throughout your project, you will need to constantly balance the constraints of time (length of time the project takes to complete), scope, and cost. Should any one of the three "triangle" components grow, there is a direct effect on the other "corners" of the triangle. Thus, as scope grows, so does the project costs and its scheduled completion time.

The project plan is a working document.

"Planning" is such a painful word in some public safety circles that the thought of creating another plan—or set of plans—may not be particularly appealing in your current quest to improve communications interoperability. On the other hand, few of us would dream of sending carpenters, plumbers, and electricians out to build us a new house without an agreed-upon set of blueprints in the general contractor's hands. Properly done, your project plan won't be one of those documents that are quickly shelved—it will be a dynamic, evolving document that is continuously used to manage the project.

Before getting started with creating a project plan, recognize that multiagency technology efforts are particularly at risk of failure. Institutionalized barriers to communications across organizations affect our ability to jointly manage projects, requiring careful and practical definition of the scope of projects, timelines, budgets, and how risks typical to technology projects will be managed. Obviously, these barriers contribute to the very "first responder" interoperability issues you're working to resolve.

Project planning improves odds of success.

The project planning process, itself, improves odds of success by bringing stakeholders to common agreement on details. It produces a detailed, actionable plan to achieve the project's objectives. A plan developed by the project manager with input from working groups and accepted by the project's Steering Committee is a powerful tool to manage the complexity of interagency initiatives.

Throughout the following, we are assuming you are or will be the project manager. Your project plan will establish the scope of what will be accomplished, set a timeline and budget, and include sub-plans for managing project risks and communicating project activities and statuses. The cyclical process of creating and maintaining one throughout the life of a project makes assumptions explicit and decisions binding.

Project Planning 101: Set the Scope and Objectives

With a firm understanding of the interoperability goals to be achieved and a broader understanding of the needs existing across agencies to meet those goals, you can now document and define the project's detailed scope and objectives. Scope planning fleshes out your charter's initial scope statement with requirements developed during needs analysis and details from the conceptual design. It provides the most basic elements of the project plan.

The three pieces of a good project plan that deal with scope are:

1. Scope statement
2. Project objectives
3. Scope management plan

Preparing for Change

Technology projects generally accompany and lead to lots of organizational change. Communications interoperability projects can lead to even more upheaval because they affect not only internal processes, but also relations between organizations. Voice and data communications are such critical tools for emergency responders, any disruption of current capabilities, in particular, threatens to cause some serious push-back on the project.

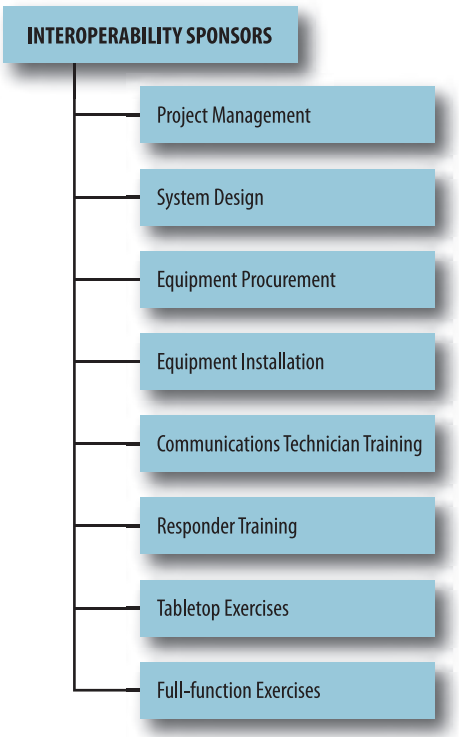
Executive sponsors: Change management is an integral part of project management. Prepare your organizations for change by requiring a formal plan that controls the project scope, budget, and timeline to achieve the interoperability goals and objectives you have set out. It should include a section on how the risks inherent in large projects, in general, and your project, in particular, will be managed. It should also include a plan for communicating progress realistically to all stakeholders, including line staff, supervisors, management, and any stakeholders beyond your organizations. Manage the expectations of your employees and make sure they have reason to share ownership of the project's success.

Follow these steps to establish your project scope and objectives:

Step 1
Draft a Scope Statement

As project manager, your first scope-planning task is to assemble a draft statement with definitions of what's in and out of the project, supporting detail for the project's business case, and the assumptions and constraints that will shape its outcomes. Be sure to include any grant requirements that you already know about. They will have a definite effect on the project.

Figure 8-1: Sample Work Breakdown Structure



The scope statement serves in this form as an incomplete working document for the next steps. Add an initial work breakdown structure[48] to describe the phases and individual activities in sequence that will take the project from conception through design and implementation to ongoing operations (see Figure 8-1). At this point, focus more on what the activities will be—their interdependencies—and how they proceed in sequence, rather than on how much time they will take. Your timeline will be set a bit later on.

48. *Work breakdown structure* is a "deliverable-oriented grouping of project elements that organizes and defines the total work scope of the project. Each descending level represents an increasingly detailed definition of the project work," according to the Project Management Institute. It is typically represented as a timeline of related activities, in sequence, and showing visible outcomes (deliverables). *A Guide to the Project Management Book of Knowledge*, 4th Edition.

Example Scope Statement

The communications interoperability project will establish one interagency voice channel for all police, fire, and EMS agencies in the county for on-scene command coordination. Interagency command communications are necessary only within a one-mile radius of an incident command post, which may be established anywhere in the county. Funding limitations suggest that complete replacement of all disparate systems in use will not be possible.

Console patching of agency dispatch channels will not be an acceptable means of meeting this need. Use of gateway devices linking existing channels or systems may be acceptable if specifically designated agency tactical channels or talkgroups are used. No new radio frequencies will be licensed.

Training and exercises for county communications technicians and all responders will be conducted.

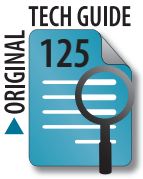
Step 2
Draft Project Objectives and a Scope Management Plan

Bring the User Committee together in a working session to take preliminary project objectives from the charter and adjust them based on the results of your needs analysis, documenting the rationale for later justification to the Steering Committee. This statement of objectives should establish specific, detailed measures of success. Use any objectives implied in the scope statement and provide additional details, if necessary.

The original *Law Enforcement Tech Guide* includes further advice on defining practical, yet measurable project objectives. For the example project above, objectives might include:

- Communications between responders for command purposes should be possible at any location within the county that is otherwise suitable for an incident command post.
- Communications should be possible within a one-mile radius of an incident command post.
- The interagency command channel should be available to responders without requiring the intervention of other personnel.

With draft objectives in hand, the project manager and User Committee can draft the final part: a plan for managing the scope. Ultimate approval for scope changes should be left to the project's executive sponsors to make sure the original vision isn't being compromised.



The original *Law Enforcement Tech Guide* provides details on the issues to be addressed in a scope management plan. Relevant statements for our example above include:

- Project scope changes must be approved by the city police and fire chiefs, as well as the county EMS director.
- Proposed limitations to the geographic availability of the command channel will be evaluated by the Technical Committee. Recommendations with estimates of cost for overcoming the limitations will be provided to the Steering Committee for consideration and comment before submittal to the police chief, fire chief, and EMS director.

Scope changes will occur. Project participants learn more as the project proceeds, affecting their ideas about what's possible. Agency needs may shift, affecting the very real definitions of what has to be made "interoperable"; or market changes may bring new technological options to meeting needs.

Your ability to identify when the project scope is changing, how it will be dealt with, and who has authority to approve changes is critical to project success.

Performance Measures

For interoperability projects, performance measures may include such things as the availability of interagency channels, the speed with which gateways are activated or deployed, the required coverage of systems linked together, and much more.

Focus on operational measures of success: the observable effects of good interagency communications. We'll have more to say about measurable improvements to interoperability in Chapter 15, **Measuring Interoperability**. Just remember: performance measures are a key part of your project plan and must be contemplated at the earliest stages of a project.

Step 3
Get a Technical Reality Check

Your Technical Committee should review the scope statement and project objectives at this point. The committee will have valuable input to assure that technological barriers, such as unachievable levels of radio coverage, haven't been inadvertently inserted into the project. The purpose for working the draft through the User Committee first is to focus objectives on operational measures of success.

This doesn't mean there aren't important technical aspects to scoping your project. Because your interoperability project will most likely involve adding new technology, the Technical Committee will have particularly valuable input on the work breakdown structure defining implementation activities and their sequence. Have the committee help establish meaningful milestones in the implementation phase to include as deliverables in vendor contracts that can be used for incremental payments.

Step 4

Get It Approved!

The final step in scoping the project is getting sign-off from the Steering Committee and the executive sponsors. Because this key piece of the project plan puts meat on the sponsors' strategic skeleton and defines what everyone will follow, their formal approval is important.

Use the occasion of presenting the scope statement, project objectives, and management plan to the Steering Committee and executive sponsors as an internal milestone to rightfully mark its importance in moving from planning to action. Note the intent to require executive sponsor or designee approval of any scope changes to keep the project focused.

Project Planning 102: Develop the Timeline

With the scope now defined in detail, a timeline can be built as the next step in project planning. It can usually be drafted by the project manager in near final form based on the definitions of activities and work breakdown structure arising from the scoping process (see Figure 8-2 on page 140).

The original *Law Enforcement Tech Guide* dedicates a chapter to this project-planning step and the material doesn't need to be duplicated here. Remember that the timeline includes not only the sequence and the amount of time individual tasks will take, but also how they're grouped into meaningful phases and further demarked by milestones and deliverables. Sound project management practices require clearly identifiable points of progress. This is most practically, often graphically, depicted in a project timeline.

Figure 8-2: Special Time Aspects for Interoperability Projects

Take into account the following special time aspects for interoperability projects:

The inherently multiagency character of communications interoperability projects requires that additional time be built into schedules for all aspects that involve formal approvals, such as memoranda of understanding and cost-sharing agreements. Agreements can take an extended amount of time, particularly as more legal review across affected agencies takes place.

Manage this time aspect by ensuring that Steering Committee members have delegated decision-making authority. Use a regular meeting scheduling process where issues requiring further internal agency review are announced prior to a meeting, presented for consideration during it, and scheduled for decision at a subsequent one. Regularly used, this structured process will help your project move steadily forward.

Voice and data communications projects, alike, are often expensive, span multiple budget and grant years, and require time-consuming competitive procurements.

Create an ad hoc committee of agency fiscal, grant management, and procurement specialists to make sure your timeline takes into account the cyclical and often time-critical aspects faced by these important partners. Their buy-in to the project can yield benefits long after the timeline is in place!

Radio projects often involve civil construction, public hearings, zoning variances, environmental assessments, permits, and licenses. In many areas of the country, seasonal weather even determines when building can occur. Every one of these aspects can throw a monkey wrench into the gears of a finely tuned timeline.

Manage these schedule killers by building in plenty of time for their completion. Start the related tasks early and pad the timeline with contingency activities that can be moved in to take advantage of delays. Carefully analyze and define dependencies between activities in the work breakdown structure to compress the timeline where possible by carrying out tasks in parallel. These techniques are all tools in the project manager's kit for dealing with such monkey wrenches.

Keep in mind that interagency projects of any type are notoriously "delicate," often depending on the leadership of key individuals and a regular supply of goodwill. Broken schedules and overdue projects strain the tightest project teams. Stakeholder frustration and skepticism can boil over when unrealistic expectations inevitably crash into reality.

Manage your project timeline well to maximize tangible resources and—more important—to maintain that intangible cooperative spirit. From the timeline submitted in the first project plan to closing out the project, the project plan revolves around the timeline. Update it regularly and keep it before the project team.

Project Planning 103: Estimate and Deliver a Budget

It's inevitable. At some point, it comes down to money.

Actually, some project managers are excited by the money aspect of their projects. There's some vicarious pleasure to be had in spending large amounts of money effectively to help public safety responders. Nevertheless, it can be challenging to be a responsible steward of taxpayers' hard-earned money. The budget portion of your project plan can be completed once the scope is defined and your timeline in place.

Costs are initial and recurring, internal and external. Don't forget that cost analysis is part of successful system life cycle planning.

Technology projects of almost any size face initial and recurring costs, incurred both within the participating agencies and through external procurements. Initial costs are all those that come about before the system is put into operation, while recurring costs arise afterwards. Internal costs are those that the project participants have most direct control over, while external costs generally come in the form of hardware, software, and services.

Cost estimation along these two dimensions is key to a sound project budget. You will probably begin by focusing on initial external expenses. As the costs of outsourcing everything from project management to radio installation start to add up, look for costs that may be covered and managed most effectively within the participating agencies. Don't make the mistake of assuming internal costs—initial or recurring—will be covered without documenting and quantifying those assumptions. From a project manager's perspective, that's a good way to get shortchanged when you turn to project partners and find they have no means of carrying their share of internal costs.

Figure 8-3: Example Cost Identification Chart

COST TIMEFRAME		COST SOURCE	
		INTERNAL	EXTERNAL
	INITIAL	Project workspace	Property
		Project management labor	Radio site infrastructure
		Remodeling of central facilities	Network infrastructure electronics
		New Intranet drops	User radios
		Overtime for training	Network management software
		Mobile radio installer labor	Controller computers and software
		Acceptance testing costs	System engineering
		Internal cost recovery fees	Construction services
			Integration services
	EXTERNAL	Physical infrastructure maintenance	Maintenance contracts and updates
		Internal network cost recovery fees	Radio site and tower leases
		Refresher training and exercise costs	Software license fees
		Technical support labor	Electrical service to radio sites
		Radio reprogramming	Backbone network services
		New fleet installation costs	Tower inspections
			Infrastructure repair
			User radio repairs and replacement

Begin by identifying the costs of which you are aware. Use a chart to categorize them according to when they'll come about and where they arise (see example in Figure 8-3).

Follow these four steps in developing your budget:

Step 1
Gather Internal and External Cost Data

Pull together cost estimates for each of the items you have identified. Often it's difficult to quantify all these costs because details are embedded in budgets spread across multiple agencies. Still, estimates are important to show contributions by all project participants even if they're made in the form of costs avoided. For example, significant initial and recurring costs for radio sites and tower space can be avoided at times through the sharing of existing facilities owned by one project participant or another.

External cost estimation is more art than science. Obviously, you're in the earliest stages of defining your project at this point and have few ideas of what will ultimately have to be purchased. Most agencies are in regular conversation with their current communications vendors and can get budgetary estimates without running afoul of procurement rules, but check with your own purchasing officials before doing so.

Alternately, you can turn to other agencies, issue a formal request for information (RFI), and even hire consultants regularly working in the field to help create budgetary estimates. The original *Law Enforcement Tech Guide* provides more information on these options.

Most grant programs being tapped today for communications interoperability projects require that local funds be used for property, towers, and permanent construction. Remember that many grant funding programs for technology will pay for up-front start-up costs, but will not pay for recurring costs. Protect your budget by thoroughly understanding all grant limitations!

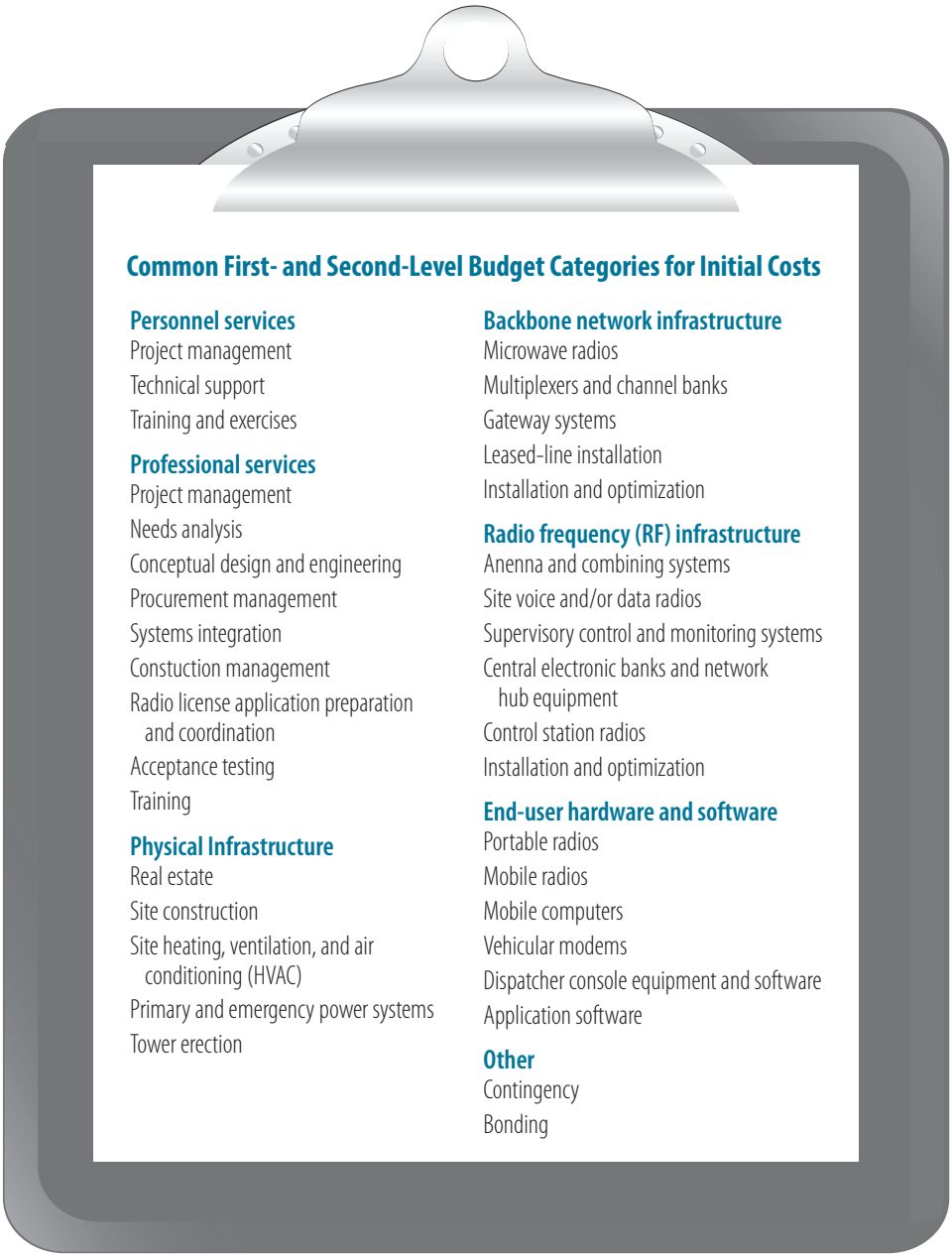
Step 2
Create a Project Budget of Initial Costs

Your budget of initial costs will necessarily include many figures, small and large, spread across the project timeline. While detail will be important later on, recognize that estimates are bound to be rough at this point. Don't create an artificial level of budget detail by including costs down to the last nut and bolt. You may know the average height of antennas above ground level at your radio sites and the going rate of feedline, but there is no sense in detailing that cost when the variance in major cost categories will be orders of magnitude greater than anything spent to connect radios to antennas.

Use a spreadsheet with low and high cost estimates for each of the budget categories you choose to use. Budget detail beyond first and second levels will become important in later, updated versions of the project plan, but this should be sufficient to move forward with your initial version.

Common first- and second-level budget categories for initial costs may be categorized as shown in Figure 8-4.

Figure 8-4: Common First- and Second-Level Budget Categories for Initial Costs



Common First- and Second-Level Budget Categories for Initial Costs

Personnel services
- Project management
- Technical support
- Training and exercises

Professional services
- Project management
- Needs analysis
- Conceptual design and engineering
- Procurement management
- Systems integration
- Constuction management
- Radio license application preparation and coordination
- Acceptance testing
- Training

Physical Infrastructure
- Real estate
- Site construction
- Site heating, ventilation, and air conditioning (HVAC)
- Primary and emergency power systems
- Tower erection

Backbone network infrastructure
- Microwave radios
- Multiplexers and channel banks
- Gateway systems
- Leased-line installation
- Installation and optimization

Radio frequency (RF) infrastructure
- Anenna and combining systems
- Site voice and/or data radios
- Supervisory control and monitoring systems
- Central electronic banks and network hub equipment
- Control station radios
- Installation and optimization

End-user hardware and software
- Portable radios
- Mobile radios
- Mobile computers
- Vehicular modems
- Dispatcher console equipment and software
- Application software

Other
- Contingency
- Bonding

A Bundle of Costs

Large radio system vendors will prefer to act as your *systems integrator*, bringing all the complex pieces of a modern communications system together. They're very capable of doing so and generally can better guarantee that their own products will perform if they do. The downside is that the service doesn't come for free and you'll probably pay a premium for commodity items that you could buy "off the shelf."

Prepare yourself to be a good consumer. Take the time early in your budgetary planning to break out cost estimates for services and subsystems. This will give you needed detail later on for the procurement process and beyond to contract negotiations.

Information is your primary tool in managing vendor relationships. Don't give away the farm by ignoring costs that can be buried in system integration and implementation services.

Step 3
Estimate Recurring Costs

Recurring costs for your project will be highly dependent on the amount and cost of new technology implemented. Today, communications systems are priced much more like computer systems, with maintenance packages offered by vendors that cover incremental software upgrades and even remote monitoring. Hardware upgrades may be necessary for certain software upgrades, much as they are with computers. If your system is as successful as you hope, recurring internal and external costs may actually be greater than initial costs.

The rule of thumb for estimating annual software and hardware maintenance contracts is 20 percent of the original purchase price. Other recurring costs, such as internal technical support, training, and site leases, can be significant, too. For example, monthly site leases for prime radio tower real estate are $1,000 a month and more. One Virginia county had been quoted $13,000 *per month* for three commercial radio sites that its vendor had chosen. It's important to have a sense early in this stage of your project if such recurring costs will be faced. (For more information on calculating recurring costs, see the original *Law Enforcement Tech Guide*, Chapter 11.)

Step 4

Plan for Ongoing Budget Updates

Just like the other part of the project plan, your budget needs to be maintained throughout the project life cycle. The original *Law Enforcement Tech Guide* points out that the entire project team needs to understand that a budget is a projection. Through regular updates, the project manager communicates this reality while providing current best estimates. As the project proceeds, adjustments will be offered and adopted or altered by the Steering Committee to ensure that its goals are met.

Project Planning 104: Create a Project Risk Management Plan

The term *risk management* is common enough in modern parlance, but the formal process of a plan to deal with risks in technology projects is unfortunately uncommon. Proactive identification and evaluation of risks is a proven means of keeping projects on track when the inevitable happens. Think of it as an insurance policy to deal with contingencies.

Risk management isn't a one-time effort, though. It starts once the project scope is defined and continues through the life of the project as phases are completed and milestones met. It's of such importance that the entire decision-making structure should be involved in creating and ultimately accepting the plan.

A four-step process for creating a risk management plan is presented in the original *Law Enforcement Tech Guide*. The process of identifying risks, categorizing and quantifying them, determining your tolerance level, and creating a response plan is the same in communications interoperability projects as it is in others dealing with technology. It comes down to understanding and preparing for problems that may arise (see Figure 8-5 on page 147).

Examples of risks in communications projects abound. A statewide project in Alaska struggled through the replacement of its entire executive sponsorship council and two project managers over a 2-year period. A large California city experienced a 1-year delay in its interoperability project when it couldn't come up with the required match for a grant. In New York, a losing vendor protested an award that was several times the agency's initial estimates, yet still one-third of the cost of its own bid. A Pennsylvania project faced serious delays when its radio tower vendor went bankrupt.

Figure 8-5: Common Risks in Interoperability Projects

Loss of key staff or participants

Loss of an executive sponsor or the project manager has the greatest impact on projects.

Loss of funding

Given the expense of communications projects, several funding sources usually have to come together to make them possible. Loss of a key funding stream or the inability to match a grant can require huge scope changes.

Bid protests

In a competitive field for high-stakes contracts, vendors are often willing to play hard for business. Bid protests can result in significant time delays.

Construction delays

Any number of events can delay necessary building. Given narrow funding windows, delays can put funding at risk.

Frequency licensing problems

Radio frequency spectrum may be one of the most scarce resources that has to be managed in the project. Licensing delays or disputes can seriously impact schedules.

Public protests

There's nothing like a new radio tower going up in someone's backyard to cause public protests.

Frequency licensing mistakes cost a Nevada agency its entire $14 million system when the FCC forced it off the air and another $10 million for equipment to operate on a pre-existing system of another agency. A Michigan agency spent $200,000 for a study to determine why migratory birds collide with its towers after being challenged by wildlife groups for not doing environmental assessments on the towers.

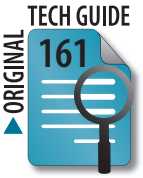
Every project will have a different set of risks, likelihoods, and impact areas, just as every project team will have a different assessment of the severity of the risks and their own tolerance for them. For example, of two jurisdictions facing difficulties obtaining radio channels, one might choose to proceed with work that can still be done, while another might temporarily halt the project to avoid putting more money at risk.

Risk evaluation and management decisions should involve the whole team.

Project Planning 105: Communicate Plans and Progress

It shouldn't come as a surprise that any project to improve interagency communications can, itself, benefit from strategies to communicate with stakeholders. The process of documenting everything from initial project meetings to the charter and beyond provides the raw materials for good project communications. It also yields the historical information that should be kept in case of personnel changes, for grant reporting, and for future project planning.

The last piece of your project plan is a formalized plan for how you as the project manager will report in various directions to all stakeholders—internal and external.



The original *Law Enforcement Tech Guide* provides an example chart showing how the variety of stakeholders can be kept appropriately informed. It describes by team member what information is needed, the amount of detail required, the frequency of communications, and the methods of delivery. Appropriately, you will have been doing a good bit of communicating along these lines by the time this part of your project plan is in place, but now's the time to formalize it.

Focus your project communications plan on getting accurate and complete, yet succinct, information to stakeholders at all levels. Each group represented in the project team and outside of it will want different information. Plans and the progress being made to achieve them will be of general interest, but from different angles. For example, upper management is much more interested in budgetary details and personnel assignments than the general public will be.

> Think like a wise man but communicate in the language of the people.
>
> —*William Butler Yeats*

The different messages have to be communicated in the form best suited to the audience, focused on their areas of interest, and in appropriate terminology. Focus general information on the operational outcomes of the project and practical matters of progress, such as phases and milestones, making spare use of technical terms and jargon.

We're convinced that traditional oral and written reports are still invaluable. Well-delivered in person, they persuade and assure like no e-mail or other electronic process can. Make the most out of your opportunities as project manager to present the project in person.

Interoperability Summit

More notes from the U.S. DOJ Interoperability Summit

Communications

- Establish a project communication plan that creates a reporting structure with and between committees and uses graphic depictions to show reporting responsibilities.
- Use daily briefings between key project team members to manage information flow.
- Keep agency public information officers informed about the project.
- Limit who communicates with vendors.

Communicating Across Agencies: The Project Website

Communications interoperability projects are challenged by the fact that stakeholders are spread across multiple jurisdictions, often separated greatly by their respective agencies' information systems. While it's not impossible to communicate well with team members who are widely dispersed, some common collaboration and office productivity tools aren't as available as they might be if everyone were in the same building.

Because of this, we've been encouraged in recent years to see growth in the use of project websites to communicate with stakeholders, including the general public. One good example that can't be done justice on the printed page is the Louisville (Kentucky) MetroSafe website (see Figure 8-6 on page 150). Louisville Metro, the area's consolidated city and county government, uses the site to provide information on its communications projects.[49]

Elsewhere, the State of Hawaii has found that web technologies can be used to create an internal network ("intranet") *portal* where employees can collaborate, create their own web pages, and otherwise share information. It's particularly interesting in that it's built from freely available software components. The State of Hawaii's Information and Communication Services Division offers a short video demonstrating the portal.[50]

There are also established secure collaboration sites supported by DHS that are free

49. See www.louisvilleky.gov/MetroSafe/.

50. See www2.hawaii.gov/dags/icsd/content/video/higovdemo_250k.asf. The State of Hawaii portal is built on the freely available open source products COREblog™, Zope®, and ZWiki™.

Figure 8-6: Louisville (Kentucky) MetroSafe Website

for the public safety community to use. These include the National Interoperability Information eXchange (NIIX) and the First Responders Communities of Practice. Registered NIIX members can access peer-created documents and share information with each other. Members can also use NIIX tools to collaborate in the creation and development of documents.[51] The Community of Practice supports improved collaboration and information sharing. Registered users can join communities that interest them and collaborate on wikis, blogs, and discussion boards.[52]

Commercial products drive most project portals that we've come across, however. Microsoft SharePoint® web collaboration software is popular in agencies that use the company's office productivity and server applications. SharePoint is easily integrated with those other applications, intuitive, and well supported by an army of value-added resellers. There are even interagency collaboration tools for incident response built on the platform.

51. See www.NIIX.org.

52. See https://communities.firstresponder.gov/web/guest.

As with any open source or commercial software of this complexity, initial setup of web portals and system administration requires trained IT specialists. On the other hand, there are an increasing number of portal hosting services. These online businesses will provide World Wide Web access to your project website hosted on their computer.

Hosted websites can be cost-effective and simple to manage.

Portal-hosting companies typically provide all the services you would have with similar software purchased and installed on your own systems and networks, although they can't easily take advantage of any internal e-mail, calendaring, and other office productivity services your agency has in place. This isn't a critical factor in choosing to use hosted portal services for interoperability project participants spread across multiple jurisdictions. Costs are reasonable too, depending on the amount of document storage, network bandwidth, and number of user licenses needed.

Portals of any type still take considerable time to configure and manage—hosted or otherwise. If that's beyond your interest, skills, or available time, there are still options. At least one agency is using the popular web service Yahoo!® and its "groups" feature for their multijurisdictional project to create a shared e-mail and chat service, file storage space, calendar, and even poll-taking capabilities.

If you need a few more project management capabilities, check out the simple hosted services at SkyDrive.[53] This file storage and sharing program provides free storage in the cloud. You can share project files with an unlimited number of participants at no cost.

Freely available web services can help with interagency project communications. See COPS Issue Brief 11–*Free Project Management Tools*, http://ric-zai-inc.com/Publications/cops-p238-pub.pdf.

53. See http://explore.live.com/skydrive-get-started.

Graphically Communicating Roles: The RACI Matrix

To be prepared is half the victory. —*Miguel De Cervantes*

One final communications technique we would like to share is the use of a *RACI Matrix*—a matrix of processes and project roles (see example in Figure 8-7). The matrix itself is simply completed by entry of the letters R, A, C, and/or I to further indicate work duties or roles for listed activities. The initials stand for:

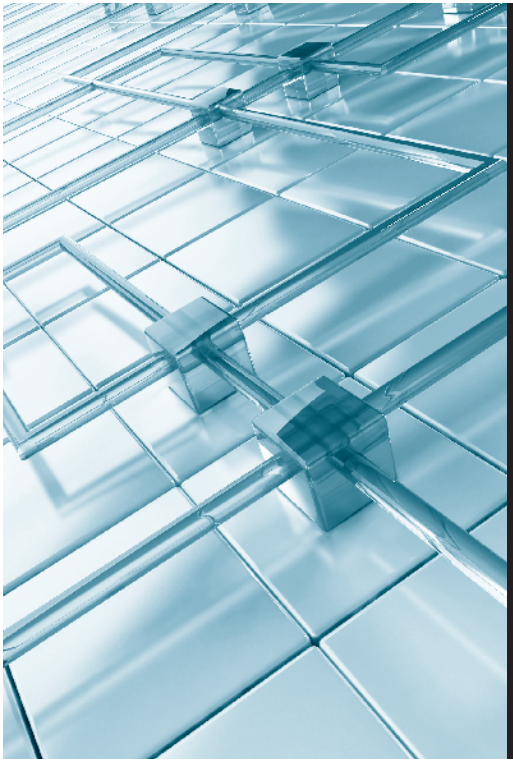
R	**Responsible**	Who does the work or owns the problem?
A	**Accountable**	Who signs off or approves the work?
C	**Consulted**	Who has information needed to do the work?
I	**Informed**	Who needs to be notified of the results?

With these five pieces in place—the **scope statement**, **timeline**, **budget**, **risk management**, and **communications plans**—your project plan is complete . . . for now! While it will surely be a good plan with all these elements, a great plan is the one that is up to date.

The work roles may be shared and an individual may have more than one. For example, the Steering Committee is broadly accountable for most project activities, but in some cases also has to be consulted in depth for further information on a subject. Implicit in the chart is that anyone accountable or consulted on work is also informed of results.

Figure 8-7: RACI Matrix Example

Activity	Executive Sponsors	Steering Committee	Project Manager	User Committee	Technical Committee	Other Subject Matter Experts	Agency Legal Staff	Agency Procurement Staff	Agency Grant Managers
Create a decision-making structure	A	R							
Create a project charter	I	A	R				I		
Assess current business processes			A, R	C	I	C			
Determine stakeholder needs		A	A, R	C	C	C			
Develop general system requirements	I	A, C	R	C				I	I
Evaluate buy versus build options		I	A, R		C	C			
Set the project scope	A	C	R	C	C				
Develop the timeline		A, C	R			C		C	I
Estimate and deliver a budget	I	A, C	A, R	C	C	C		I	C
Create a risk management plan	A	A, C	A, R	C	C		I		
Communicate plans and progress	I	A	R	I	I		I	I	I



CHAPTER 9

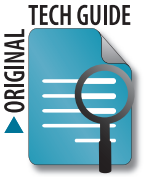
Acquire the System Components

What: System acquisition requires a structured, iterative process for acquiring the services and physical components to create an interagency communications system, whether voice or data.

Why: Communications interoperability usually requires new or additional systems that have to be designed and procured. A well-organized process can avoid wasted time, money, opportunity, and foster goodwill between partners who are dependent upon cooperation.

Who: The project manager is at the center of system acquisition. Members of the Steering Committee serve in additional roles, as do members of the working committees. Special ad hoc teams are often necessary for legal, community relations, and procurement assistance.

When: Acquisition occurs once needs are defined and the initial project plan is created. It proceeds through design and functional specifications to procurement and contracting.



How is communications interoperability different from other types of technology projects? It's rarely recommended that agencies create their own computer-aided dispatch (CAD) or record management system (RMS) software, from scratch. It's inevitable that communications interoperability and information sharing projects require lots of detailed design and engineering. As with any kind of technology project, multiagency efforts naturally add layers of complexity through complex interaction of needs, financial abilities, and procurement rules.

This chapter builds on the original *Law Enforcement Tech Guide's* Part IV, **Acquiring the Technology**. Chapters 14 and 15 of the original *Tech Guide* provide procurement and contracting advice that will serve you well in your project. We won't rehash those equally applicable details here, but instead will focus on the unique aspects of interoperability systems acquisition. Be sure to read and use the *Tech Guide's* advice!

Public safety technology projects, in general, and communications interoperability projects, in particular, are put at severe risk when they are approached merely as a procurement exercise. The complexity of these projects requires an organized, structured process for proceeding from the needs you've collected to a detailed design and on to the often-expensive process of acquiring services and the physical parts of your system.

There's a direct correlation between how rigorously this phase of your interoperability project is approached and its chances of success. **Even if a large share of the technology to improve interoperability between agencies will be purchased from a single vendor, a solid process of defining, designing, specifying, and buying the system is needed to manage both the project *and* the vendor.**

One key way to manage such complexity is through iterative steps of design, procurement, and implementation. Through a process of decomposing the work to be done, more detail about the "system" is developed. All stakeholders learn more about the components of the system and how they fit together. This progressive process allows the project to be broken down into manageable pieces—some may be executed entirely by the participating agencies and others through the help of communications systems vendors and service providers.

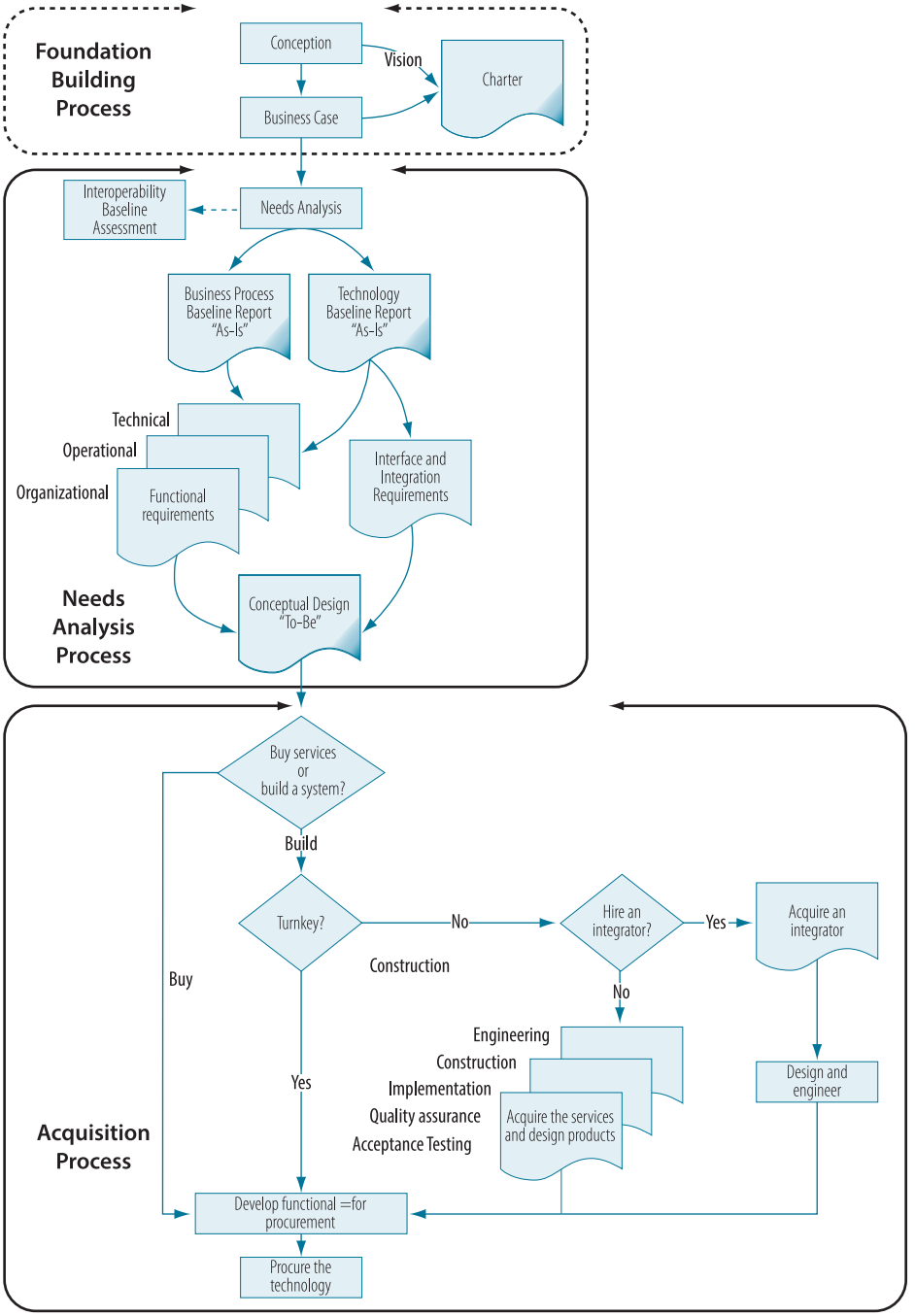
Assumptions: We have to make some assumptions about your project. Not all interoperability initiatives require massive system changes or new equipment purchases. Your project may be focused on the simple process of swapping radios between agencies during an incident so each may talk to the other. It may be to program channels commonly available between agencies in everyone's radios. Here we're looking primarily at projects that eventually require that some additional or new technology infrastructure be put into place.

Both voice and data systems follow the processes described here, though with data systems there's also an additional effort to find and implement software applications.

The process diagram (see Figure 9-1 on page 157) depicts the steps that have been recommended that would lead your project up to this point. It shows the progressive process of system development.

If they didn't seem so before, the processes have to seem daunting now! Don't worry. We will break down the work needed to get from beginning to end into steps and decisions to be made along the way.

Figure 9-1: Design and Acquisition Process



It's tempting to turn the checkbook over to the first vendor who offers big promises to solve your interoperability problems. Don't do it! As we've been saying all along, interoperability isn't primarily a technology problem. There are many organizational, operational, and technical function changes to be made to improve interagency communications in most regions of the country.

A final note before we get down to it: improved interoperability results from improved communications (in both technical and nontechnical senses) and cooperation. It truly requires a system of related technical and nontechnical systems. The system definition and acquisition phase of your project is one requiring particular attention to managing relationships—not only between your operational partners, but also with the communities being served by and paying for this initiative, as well as the equipment and professional services vendors you'll need to partner with.

Manage the relationships. Don't let the new system of systems ever become a divisive influence, which happens when participants lose sight of the goals.

System Acquisition 101: Groundwork

Any sufficiently advanced technology is indistinguishable from a rigged demo.

—*James Klass*

There is a bit of groundwork to be laid before moving into actual acquisition of system components. Not every project will require all the work we'll discuss, but large voice or data systems require most, if not all, because of their complexity. Indeed, if your needs analysis discussed in Chapter 6 led to a decision to simply buy services to improve interoperability, as opposed to building new systems, then you're moving directly to the procurement steps described near the end of this chapter and in added detail in Chapter 14 of the original *Law Enforcement Tech Guide*.

Generally, you move into the acquisition phase of your project by first understanding relevant procurement and contracting rules and how the project teams will be structured and staffed. Through these steps, you'll move from a conceptual design to procurement and contracting.

Step 1
Research the Rules

Moving into any procurement, project decision-makers need to be aware of the rules that govern it. The project manager bears particular responsibility. This can be quite a challenge in large interoperability projects that span organizations, jurisdictions, and sometimes even state boundaries. They are increasingly funded through a complex mix of grants, tax revenues, and fees that bring special challenges to management of the project budget. Not only do funding stipulations limit what can be purchased, under which processes, and in particular timeframes, but they also limit how ownership can be shared across organizations. It's easy to imagine how difficult agreements between jurisdictions can be when joint or equitable ownership of shared system components for interoperability is impossible.

Don't work yourself into an acquisition corner by failing to understand your agency's purchasing and contracting rules, as well as those of your partners.

There is a way to deal with the complexity: get help!

We'll touch on the array of teams that may be needed in a moment, but you can start by creating an ad hoc team of financial advisors from purchasing staff in each of the key involved agencies. With their help, create a broad plan on how to meet all agencies' rules or, alternately, the project's goals and objectives through financially discrete procurements. For example, it may be clear that one set of rules applies across the partners or that a couple key participants in the initiative can take on all purchasing responsibility.

Before deciding how to proceed with system acquisition, consider that large procurements can rack up significant internal costs—up to 5 percent of the system cost.

Today's competitive procurements are so technologically and administratively complex that they require advice from a multiplicity of sources, including legal counsel and financial advisors. There are very real costs for this, too—as much as five percent of the procurement, in our experience.

—Steve Proctor
Executive Director
Utah Communications Agency Network (UCAN)

Step 2
Form the Teams

With an idea of the amount of work involved and what share will be accomplished internally, create the teams to carry it out. Consider and select members from across the participating agencies as broadly as you can. This requires knowledge of individuals and their abilities that you, the project manager, may not have. Turn to Steering Committee members to help find talent from among their agencies. Talking with them also provides the opportunity to get their agreement to commit staff time to the project.

All or none of these teams may be necessary, depending on the size and scope of your project. Keep in mind that project participants can wear multiple hats—if they're not already!

Two working teams are particularly useful at this point: the procurement and policies/procedures teams.

☐ Procurement Team

A suitable proposal evaluation team for a turnkey procurement would be composed of the same members, but include fewer of them.

Presuming there will be some purchase of services or technology for your project, create a procurement team that will take responsibility for shepherding the process through selection of a procurement method, specifications development, proposal evaluations, vendor selection, and contracting. The team may bring in expertise for particular tasks—such as additional operational experts for developing functional specifications or legal counsel for contract negotiations. However, they have a central role to provide continuity through the entire process.

Select members who have some background with purchasing. The ins and outs of navigating a significant procurement aren't skills most people are born with; they come from experience. Ideally, that comes with real operational experience of using communications equipment as emergency responders, too.

☐ Policies/Procedures Team

How agencies will work together drives many procurement functional specifications.

The second team that can be kicked off right away is one to collect and meld policies and procedures between partnering agencies. Start this process early because the learning process involved can impact functional specifications for any procurement. For example, if the agencies have or want a policy stating that a dispatcher must always be at the control point for connecting agency channels physically or logically through a gateway device, that establishes a functional need to be specified. Alternately, if they would require that a communications unit leader (COML) or a communications technician (COMT), as defined under the Incident Command System (ICS),[54] be deployed during incidents of a particular size or larger, a transportable gateway may eventually be chosen in response to that functional requirement.

Clearly, the procurement and policies/procedures teams overlap. They may share some members, but define them separately and have their work proceed in parallel—both to make the most of available time and because the work does not *completely* overlap.

54. The Incident Command System, a key part of the National Incident Management System (NIMS), will be discussed further in Chapter 12, **Develop Policies and Procedures**.

Make a Note of It!

In order to keep your project focused on improvements in operations, limit vendor access to team members. If necessary, use an agreement for individual team members requiring all vendor inquiries to be directed through the project manager or designee. Don't risk team members becoming advocates for particular technologies!

Other teams may be necessary through the acquisition process. Set these into motion depending on what work you choose to take on internally and what you intend to contract out.

☐ Engineering Team

Whether or not you contract for system design engineering, consider establishing an engineering team, typically composed of those involved in the Technical Committee. These people will either be responsible for or guide the engineering necessary for radio projects much larger than a single voice repeater or wireless data access point. Even in projects making new or additional use of existing systems, there is often an engineering and optimization aspect involved that requires technical steering. In the procurement process, the engineering team plays an important role in establishing technical specifications, eliminating those that unnecessarily limit choice, and serving later in the evaluation process.

Select Team Members Carefully

In our experience, one key quality of a good project manager is the ability to pick the right people for the right teams. Not all potential project participants have the people skills necessary for good teamwork. Be careful with the engineering team; some of the most technically adept technicians struggle in teams. Select members for the engineering team who have no preconceived notions of the "best" technology and who work well with their peers in other agencies. Avoid dogmatic members of the engineering team—or any team for that matter!

☐ Construction Team

Look elsewhere in the participating jurisdictions for civil engineering and construction expertise.

As you might guess, a team to deal with the peculiar design, procurement, and implementation aspects of new physical facilities isn't necessary in all projects. When it is, the skills of members are distinct. We'll touch on the civil engineering aspects of some projects in the next section, but not every interior designer is qualified to excavate for a foundation or frame up a house.

In addition to Technical Committee members who will have your best institutional knowledge of currently used and other potential facilities, look to your jurisdiction's construction and building divisions for further expertise. In many cases, the construction team has to oversee the work of contractors selected specifically for site development, permitting, and navigating zoning mazes.

☐ Public Relations Team

We looked previously at the importance of communicating with the public about your interagency project to improve critical interagency communications. In the acquisition phase, community relations are critical when you start building new facilities. Try to put up a tower near an elementary school and learn a bit about "contract negotiations"!

Turn to individuals within participating agencies who already serve this function. It requires another distinct skill set and persons already doing the work no doubt already have contacts and procedures for dealing with a multitude of community relations issues. Your Steering Committee members may also be in management positions suitable to help in this regard.

☐ Acceptance Team

Use key members of other project teams for the acceptance process.

We're all looking for acceptance, right? Well, maybe so, but in the acquisition and implementation phases, *acceptance* is the process of using mutually predetermined measures between contracting agencies and contractors to determine when work has been successfully completed. While this is naturally seen as an activity taking place well into the process of building systems, there are at least two reasons for setting an acceptance or quality assurance team into motion early on.

First, conditions for acceptance of work, whether services and/or technical implementation, should be spelled out in the procurement process. Your vendors are going to make sure they are spelled out in one form or another. It pays to go into the procurement process with clearly defined measures of what successful completion of an engineering design, construction management, or system optimization will be.

Second, the acceptance team can be seen as providing a *quality assurance* function. In the world of technology project management, quality assurance is the recurring process of guaranteeing in each phase that a project's objectives are being followed and incremental measures of quality are being met. Ultimately, given the tools developed through early project definition, conceptual design, detailed design, and functional specification, the acceptance team also functions in this role.

Quality management is a distinct responsibility of project managers and is sometimes outsourced in large projects.

The Head Coach's Challenge

If you're the project manager of a sizeable interagency communications project, you may be looking at this list of potential teams beneath the carefully crafted decision-making structure you've already created and think the project might drown in a sea of organization charts. Don't despair! While formal and ad hoc working teams are brought together to do specific, task-level work, they're often composed of the same project participants—often most from the project's standing committees.

Your project management challenge here is to help team members understand that they'll wear different hats while working in separate teams, but the team's purpose is to take a focused task and carry it to completion. Distinguishing specific teams emphasizes distinct areas of work to be done and helps participants navigate the maze of tasks involved in large technology projects.

Manage the project's timeline by carefully having these teams work in parallel to one another. Clearly, the amount of overlap between members is going to affect how much can be accomplished by them, but good project managers compress timelines by having work done in parallel as much as possible.

System Acquisition 102: The Art of Procurement

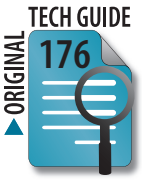
Throughout the previous sections of this chapter, we talked about the work to be done to acquire a new system for improved communications interoperability. Understanding what has to be accomplished and how to organize the work will guide how you procure services and equipment. As we've mentioned, a detailed examination of what's involved—to the extent of designing a good share of the system—guides your decisions on what tasks can or should be done internally and what needs to be contracted.

The original *Law Enforcement Tech Guide* provides valuable information on the subjects of procurement and contracting. The guidance found there is applicable to a variety of communications, interoperability, and information sharing systems. We will step through its guidance in the following pages, referencing specific locations for your broader review.

If your project is large or complex, you may have already chosen to contract out some services. Systems design, integration and management services, and site development can account for half or more of some systems, but for most projects, the largest procurement effort is for equipment. Costs include its purchase, installation, optimization, training, and initial operations.

The procurement process proceeds through four steps: selecting the right procurement tool, developing functional specifications, building criteria for evaluation of expected vendor responses, and executing the process.

Step 1
Select the Tool



The most common procurement tool used for communications systems is the request for proposals (RFP). The tool under one name or another is available to all jurisdictions. It allows you to state requirements and functional specifications, and then allows interested parties to propose solutions. The RFP is distinguished from an Invitation for Bid (IFB) in the flexibility it allows vendors to propose solutions for evaluation and the agency's ability to negotiate costs based on what they learn.

The request for information (RFI) is occasionally used by agencies in communications systems procurement, particularly to learn about technologies that can be considered. The RFI process is less formal and time-consuming than an RFP because they aren't complete replacements for one another. An RFI may lead into a negotiated procurement, but is most appropriately used to collect information for the more formal process. In the rare cases where the RFI yields enough information to conclude there is a single, suitable approach, your procurement rules may allow you move to actual procurement.

Step 2
Develop Functional Specifications

We have talked about the need for functional specifications for acquiring interoperable systems. In the procurement phase, these specifications are put to paper in a form that will encourage thoughtful, often innovative proposals, yet allow you to evaluate whether the proposed solutions will meet your needs.

The degree of specification will hinge on how you've chosen to proceed with the project. If you've chosen to go for a turnkey system, then functional specifications will be limited to operational aspects of how the system will be used and managed. If you've chosen to bring in a systems integrator independent of equipment manufacturers, you will have a standard set of specifications from the integrator to work through and select from.

Functional specifications naturally flow from the organizational, operational, and technical requirements developed in your needs analysis phase. The original *Law Enforcement Tech Guide* provides further guidance on how specifications for the procurement are chosen and worded.

Sole-source Procurement

While it's often tempting to go straight to a single source based on what you already know about a particular communications system, recognize that there's great value in maintaining competition and options in any procurement. Use them to your advantage. Don't rely on expected goodwill alone to deliver your agencies the best options at the best prices. Recognize that grants place significant additional procurement burdens on any sole-source purchases they are used for. See the original *Law Enforcement Tech Guide*, page 178, and/or the *Law Enforcement Tech Guide for Small and Rural Police Agencies: A Guide for Executives, Managers, and Technologists*, Chapter 5, **Understanding Procurement and Contracting**, www.search.org/files/pdf/SmallRuralTechGuide.pdf.

Step 3

Build Evaluation Criteria

Criteria for evaluating proposals and selecting the winner likewise flow from your specifications. They also arise from the value your agencies place on other factors. For example, your functional specifications may not have anything to say about the vendor's qualifications, but experience, stability, and record of success are key criteria for evaluating communications system vendors that will provide critical technology for your interagency communications needs.

Hopefully, the operational needs you've outlined and the functional specifications you've stated will lead to evaluation criteria that are carefully aligned with your agencies' standard operating procedures (SOPs) and incident response plans. For example, your policies/procedures team may have brought requirements to the table as to how the system has to work. They may have brought specific functional requirements for how a piece of equipment works, its electrical characteristics (such as "Intrinsically Safe" portable radios for use in potentially explosive atmospheres), or other physical characteristics. It's also possible your agencies have performance standards for particular work, such as the amount of time and effort required of dispatch to set up a patch between two channels or for a call-taker to answer a 9-1-1 call routed to a secondary emergency medical services (EMS) public safety answering point (PSAP).

These SOPs and elements of response plans should guide evaluation criteria. Other examples of appropriate criteria and how they are presented are included in the original *Law Enforcement Tech Guide*. These criteria are carried into a weighted evaluation process where particular, predetermined factors are accorded greater value than others based on your own sense of what is important.

Step 4

Carry Out the Process

Whew! With all this work out of the way, it's actually time to carry out the procurement! Unless you've been involved in similar projects before, the amount of work involved in getting to this point may have come as a surprise. Trust that it's all important to get you where you want to be: better interagency communications through your voice and data systems.

Your jurisdiction's procurement rules, those of partnering agencies, and those brought as conditions of other funding sources, determine the actual steps taken to release the procurement, await responses, collect proposals, step through evaluations, and make a selection.

Cost is bound to be one of your greatest considerations, of course, although RFP rules for most jurisdictions don't require that it is necessarily the predominant factor in making a selection. As a matter of fact, that's a key reason why you created detailed evaluation criteria. It's not uncommon for cost to be half of the total points accorded proposals for radio systems.

Recognize that prices can be brought down 5 percent, 10 percent, and even more through negotiations, which we will talk about next. Through a formal and detailed procurement process, you will get sufficient information in response to your RFP to decide how to proceed, even if the total proposed cost is well beyond what you expected. Believe us, it happens!

Though you may have to go through a process known as "best and final offers" to further winnow down the selection, eventually you get to the point of identifying an apparently successful proposal. This will lead to negotiation of one or more contracts.

System Acquisition 103: Create the Contract(s)

You're almost ready to move to implementation, which is what you have probably been anticipating since being asked to take on this project. However, the contracting process is perhaps the most delicate part of your entire project, so proceed carefully. **It's entirely possible for a poor contract not only to put your whole *project* at dire risk, but also the money, work, and goodwill agencies have brought to the project up to this point.** Don't risk everything by either forcing through a bad contract or accepting one out of haste.

The original *Law Enforcement Tech Guide* dedicates an entire chapter to this subject. It is entirely applicable to your interoperability project. We're not going to repeat its good lessons here, although we do have a few tips to pass on when it comes to dealing with these specific types of projects.

Learn to negotiate or use professionals. It surprises us to see law enforcement agencies that are adept at the very serious process of hostage negotiations simply cave in when it comes to negotiating with technology vendors! Take the contract negotiations process seriously and turn to professionals, if necessary, to look out for your best interests.

Know your vendor. More than other types of information technology, radio systems are dominated by relatively few vendors. While this limits your options in some cases, it does provide better opportunities for understanding them. This provides for both better management of the project on your part and negotiation of contracts, in general.

Know your vendors' marketing and sales cycles.

Find out all you can about vendors' marketing and sales cycles. All have particular strategies for product life cycles and managing sales. These strategies affect how you will deal with the vendor, hopefully to your advantage. Since they will most certainly affect the cost and capabilities of your system over time, it pays (literally!) to know about them at this point in your project.

In real estate, there are "motivated" buyers and sellers. From the contract negotiation standpoint, it's invaluable to know your vendors' "motivations." The sales staff assigned to your procurement will undoubtedly be paid in part on commission. The amount of your contract has a significant impact on what they, personally, take home through the contract.

Vendors prefer penalty clauses to bonding requirements that increase costs even for successful projects.

A common motivation of all vendors is, of course, maximizing profit and avoiding costs. One they prefer to avoid is the hard cost of bonding. Your agencies' procurement rules may require it, but vendors would much rather be compelled under contract by penalty clauses than bonding requirements because they can avoid costs by carrying out the contract well—which is in both parties' interests. Any invocation of penalty clauses typically gets lots of attention through a vendor's chain of command. Knowing that the vendor's staff are subject to that level of scrutiny can be useful during implementation.

In the process of managing the project, any situation that requires invocation of bonding clauses and collection on the agencies' part ultimately removes the ability of the respective agency and vendor project managers to negotiate. Do all you can in managing the project to avoid ending up in this circumstance.

Prepare to transition maintenance of the technology. The larger your project, the more likely it is that you will enter into some form of maintenance agreement with your vendor. If you plan on maintaining some or all the system yourself, recognize that vendors that offer maintenance services have a natural interest in selling those services. Carefully define maintenance responsibilities and any eventual transition of responsibility to your staff. Include specific language in the contract about expected skill levels of staff to maintain the system if the vendor provides that training.

Use your knowledge of the vendor's sales cycles to negotiate the best deal. Typically, better deals can be made if you time the proposal release, evaluation, and award cycle to mesh with the calendar year. Contracts signed in December often yield the best prices because vendors and sales people are nearing the end of the tax, corporate reporting, and sales commission year. They are typically more motivated to sell at the end of calendar quarters, especially the end of the year.

The best deals can be negotiated in December. Equipment prices can vary by five percent based on the time of year.

Recognize that vendors do not want to come back to the bid table multiple times if they can include more under a larger procurement. Some large systems' vendors pay commissions based on "tonnage"—the total cost of the procurement. They also have more pricing flexibility on soft costs. It may seem odd, but the cost of the system and its profitability to the vendor are only loosely related. The effect is that in negotiation, you may be able to get concessions on more profitable items in exchange for ones with less "mark up" as long as the bottom line isn't greatly affected.

Recognize how quotes are assembled. Look for costs that are added as extras or that could potentially be done by someone else. An example is training. There is often flexibility built into these cost quotes, with the potential for good profitability on the vendor's part. Consider if you really need their particular training for all proposed aspects and be prepared with the costs of alternatives when you go into negotiations.

Vendor-provided training can be very expensive—check quotes carefully.

Similarly, look for costs that are split out separately, but couldn't possibly be contracted separately. Our favorite example is system installation, configuration, and optimization. While it's logical to use these as separate milestones for payment, for most systems it's hard to separate them out as independent tasks that could be accepted or rejected in the contract negotiations process.

Recognize your vendors' internal processes. For better or worse, large commercial organizations have a lot of bureaucracy. Sometimes this can work to your advantage. First, so much of contract negotiations has to do with the vendors' and the agencies' internal rules of procurement that there's a lot of work to be done between contracting professionals and legal counsel. Don't use a lot of your procurement team's time and energy in that process; break it out as separate work in actual negotiations.

Second, recognize that the vendor's bottom line profitability on your project may not be affected by concessions their project manager is able to make. For example, at least one manufacturer of equipment has a standard markup on portable radios of approximately 10 times. That is, the retail cost will be approximately 10 times the cost of manufacture. During the project, the vendor's project managers are afforded the ability to bring additional equipment to the customer to compensate for delays, disputes, and the other typically unpleasant details of projects. However, they may have less flexibility on changing the standard markup.

To avoid invocation of penalty clauses, vendors may provide additional equipment at cost.

It's particularly valuable for you to know if your vendor accounts for this cost in the project's bottom line at retail or at the cost of manufacture. At least one large manufacturer accounts for it at the cost of manufacture and without significant impact to the project. This provides the vendor's project manager great flexibility in avoiding penalties that may be built into the contract.

With any luck, you will get through negotiations with an agreement that keeps both your project and the vendor's interests intact. The contract will be the basis for much work yet to come, so make sure it serves your purposes and gives you the project management leverage you need to succeed in successive steps.

CHAPTER 10

Implement the System

What: System implementation is the process of installing, integrating, testing, and accepting procured technology. Training users and support personnel is key to integrating technology into agency response procedures.

Why: A formal implementation process provides all project participants, including vendors, a clear blueprint for building an interoperable system of systems. Failure to follow an implementation plan leaves the procurement and entire project at risk of failure through miscommunications and divergent expectations.

Who: The implementation plan is created by the project manager in cooperation with the vendor's project team and through further effort from working groups. The Steering Committee reviews, approves, and submits the plan to executive sponsors for final approval before implementation begins.

When: Formal implementation starts as soon as a contract has been negotiated and project teams are in place.

Part V of the original *Law Enforcement Tech Guide* addresses implementing technology acquired through the preceding procurement phase. The format and elements of implementation plans are dealt with in-depth in its chapters, as is acceptance testing. Here, we will address specific aspects of implementing communications technology for improved interagency communications and its integration into existing systems.

Chapters 16–17 of the original *Law Enforcement Tech Guide* cover the implementation process in technology projects.

Implementation is the most exciting time for project managers. Many plans and much work comes together during implementation to actually improve communications. Up to this point, there has been a lot of envisioning, but few tangible results outside of paper. Implementation is the time when technological and operational pieces come together to create systems.

Prologue to an Implementation

Implementation of the system of systems we have described requires that you, your vendors, and your project teams all work together toward well-defined ends. In the implementation phase, definition of those ends requires clear roles and responsibilities, an implementation plan, detailed documentation, and an acceptance test plan. Because the value of any system is directly related to how well it is used, training according to established or newly created procedures is a critical part of implementation.

Further Define Roles

The implementation process has two sets of roles: yours and the vendor's. This final phase of the project really does entail a partnership. Previously, you managed vendor relationships from a distance to keep the focus on operational outcomes of the project and to protect the integrity of the process. Now is the time for their efforts to bring technology to your interagency communications needs.

How you approached procurement drives implementation. If you contracted for a turnkey system, most responsibilities have been left to the vendor. If, on the other hand, you chose to handle system integration yourself, the implementation plan will contain many more tasks for you and the project teams.

☐ Your Roles

Vendors become stakeholders once contracts are signed.

As the project manager, consider yourself the CWO (chief wellness officer). You're responsible for assuring the project is well-founded, well-defined, well-planned, well-communicated, and now well-implemented. Consider that in this phase you have new stakeholders: your vendors. Obviously, their stake in the project is clear, but like other stakeholders, they depend on your success in carrying out these responsibilities.

You have one primary and three oversight responsibilities in implementation: creating the implementation plan comes first, followed by oversight of documentation processes, acceptance testing, and training. Of course, you also have the ongoing role of managing the project in its entirety. As we've mentioned, that entails continued communications with stakeholders, managing timelines, budgets, and scope, and now contract management. If it seems like a big job, well, it is!

Your **implementation plan** details how the project's work is going to get done. That requires a number of decisions about who takes care of what. While you may be tired of plans by now, rest assured that most of the work for the implementation plan is already complete. We will talk further about creating the plan in the next section.

Documentation should be planned and managed throughout a project. In the implementation phase, documentation created by vendors and your project teams will serve project goals long after the system is up and running. Your added project management role during this phase is to oversee its completion.

Acceptance testing is the process of verifying that components and the system, as a whole, function as specified. You may have considered requiring an acceptance test plan as part of the request for and evaluation of proposals. We didn't recommend it earlier because most procurements for communications systems proceed as RFPs, which implies that a good deal of flexibility in proposed solutions is allowed. Acceptance plans may be very different across solutions offered, making them difficult to comparatively evaluate.

We do recommend, however, having vendors develop acceptance plans as an early deliverable. They can be built in parallel to creation of the implementation plan. Details to be considered and some examples are presented later in this chapter.

Training is absolutely critical to successful implementation of any technology. Too often technology is bought and left underutilized due to a lack of training on it for users and those who would maintain it. It is the project manager's role to include training into the implementation plan. This includes training for both technicians who will maintain the systems and for users who will put it to work.

Training is the key to successful implementation.

☐ Vendor Roles

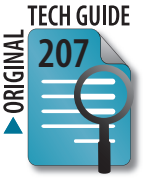
Your vendor or vendors will appropriately participate in creating the implementation plan. Their roles will have been made very clear through execution of contracts, but further details of work will be left until now to establish. There are further tasks to define, activities to coordinate, and resources to schedule.

Details of vendor work will be set primarily by your contracts.

Of course, the central vendor role is to install, customize, and activate the technology it is providing. Since you may have contracted for other vendor services, such as engineering and quality assurance, roles between vendors are important to define in the implementation plan.

Both you and your vendors have roles in implementation planning.

Establish the Implementation Team



As discussed in the original *Law Enforcement Tech Guide*, the implementation team consists of both your project manager and those of the selected vendors. In effect, they have their own projects that now intersect with yours. Remind the team, if necessary, that there is *one* central project—yours.

Other teams may be needed for different parts of the implementation. Common ones include policies and procedures, construction, training, and acceptance. Depending on your project, these and other working teams may be needed to focus work where specific expertise is needed.

There's no need to create separate teams just for the sake of creating teams. Do so to maintain a reasonable span of control. Management texts stress that, as a rule of thumb one manager can oversee three to six direct reports. As project manager, you have demanding communications roles in all directions, so don't make the mistake of failing to delegate work through teams when needed.

Your Steering Committee and executive sponsors are ultimately part of the implementation team. The Steering Committee should play an active role in reviewing the implementation plan and evaluating contractor performance. Executive sponsors must approve this very critical plan and make the final acceptance. In most agencies, final signoff on incremental payments for large contracts will be required of agency chief executives.

Create the Implementation Plan

As you might guess, the implementation plan is central to, well, implementation. You'll be pleased (relieved?) to know that we suggest using parts of other project documentation completed in previous steps to populate the implementation plan. This plan will mainly be a collection of parts from previous work brought together in a focused format for implementation.

Implementation Plan Elements

The original *Law Enforcement Tech Guide* lays out a basic implementation plan that is fully useful for voice and data interoperability projects. It suggests organizing the plan into four chapters that summarize the project, laying out its organization, the implementation management process, and then details of work, schedule, and budgets.

The varying aspects of communications interoperability projects bring additional plan elements. Figure 10-1 lists the standard topics of each chapter.

Figure 10-1: Implementation Plan Outline

Chapter 1 Project Summary	Chapter 2 Project Organization	Chapter 3 Management Process	Chapter 4 Work, Schedule, and Budget Tools
Overview Definitions Deliverables Audit trail	Plan approval process Organizational structure Responsibilities Relationships between vendors System management transition	Project objectives Assumptions/Constraints Risk management plan Staffing plan	Select contract exhibits Logistical considerations

☐ Project Summary

This first chapter of your implementation plan includes a simple **overview** paragraph, **definitions** of key terms that could be misinterpreted, and a list of **deliverables** taken from your contracts. The overview and definitions could be taken from your procurement documents as well, if you previously fleshed out an RFP or RFI in that level of detail. Include an **audit trail** block at the beginning of this chapter to log changes to this document over its lifetime.

☐ Project Organization

The second chapter details the **plan approval process.** Address how it is approved initially and how changes will be managed through implementation, with a statement of authorities and responsibilities. The approval process can be lifted largely from your project plan.

Address how project changes will be requested and approved. Clearly describe the approval process for change orders! An unmanaged change process can result in the distortion of original plans as changes creep into projects. One of our favorite project managers refers to change orders as *ka-ching orders*—as in the sound of a cash register racking up another sale. You'll want to manage project changes carefully during implementation because they will have an impact on the project's timeline and/or cost.

Clearly describe the approval process for change orders!

Remember that you have new players who will also need to know your project structure. Provide them with your **organizational structure** for this phase, adapted from the project plan. Include the vendors' organizational charts for the project as well.

Describe implementation team member **responsibilities and roles**, including those between various contractors, if more than one is used. As mentioned in the original *Law Enforcement Tech Guide*, carefully lay out **relationships between vendors** and responsibilities for subcontractors as defined in your contracts.

Conclude the project organization chapter by addressing **system management transition**. Describe how a transition of responsibilities from the vendor(s) to your team will occur. Computer and radio systems of ever increasing complexity go through a cycle of installation, integration, and optimization during which vendors initially take all responsibility for system management. That responsibility is transitioned to your staff or whoever will manage it over time—sometimes another contractor, such as a regional radio service company. The transition process should be documented here.

☐ Management Process

Use the third chapter to document details of how the project—and this phase—will further be managed. Pull the **objectives** from your project plan for inclusion here. They serve to inform others in the team what is being accomplished through this implementation of technology.

Also include **assumptions and constraints** from your project plan with any changes that have arisen through the procurement process. For example, the proposed system design may have required compromises on coverage in order to remain within the project's budget. This would lead to constraints on original objectives that will change acceptance tests.

If you've followed our recommendations, you will be able to insert an up-to-date **risk management plan** in this chapter from your broader project plan. It's fair to advise all team members, including contractors, what you have considered as potential risks to the project, how serious you consider them, and what your strategy is for dealing with them. Include appropriate information out of your contracts on any penalties clauses and dispute resolution processes.

The final piece of this chapter is a **staffing plan**. Include information consistent with your project organization chart that shows who will be assigned to various tasks during different periods. Because the timing of your personnel resources for meeting with contractors, escorting them to radio sites or other secure facilities, conducting acceptance tests, and such will be heavily dependent on vendor timelines, you will need firm commitments from vendors before being able to document your own timeline.

☐ Work, Schedule, and Budget Tools

The final chapter of the implementation plan is dedicated to the details of work to be accomplished. If your contract is with an established vendor and the project is of any significant size, this detail will have been negotiated prior to signing contracts.

Include here **select contract exhibits**, such as the initial project schedule, the budget and payment schedules, and an outline of the acceptance testing process. Keep in mind that not all members of the implementation team will have ready reference to actual contracts, so it is useful to include these items in the guide that they'll be using.

Since acceptance testing can be a very detailed process as we discuss in the next section, an outline here will serve to describe it for the general understanding of all team members.

Unless you are proceeding with a turnkey implementation, use this opportunity to define the process of handoff of responsibilities between vendors. Add milestones in your project schedule describing these events. For example, a consultant hired to prepare an engineering design will go through a draft, review, and finalization process with you before the design is handed off to contractors to build the systems.

Conclude this chapter and the implementation plan by addressing **logistical considerations** that will be faced. Large voice and data projects can involve a lot of equipment that needs to be shipped to various sites. The logistics of who, when, and where equipment is received, inventoried, stored, and eventually staged for installation are important details for a smooth-running project. Take the time to deal with these details now before you get behind the curve.

Budget Tip: The Final Payment

Contractors will appropriately expect to be paid for labor and materials as parts of the system are accepted. Part of your duty during contract negotiations was to arrange fair compensation for work while protecting the agencies from paying for an incomplete product. Payment milestones should be linked to acceptance and at least 10 percent of the contract should be held until after final acceptance. This prevents implementations from dragging on when there is only a bit more work necessary to have a functional system, as specified by the contract.

Budget Tip: Beneficial Use

Use of multiple vendors requires additional handoff milestones in the project timeline.

Contractors will also appropriately expect to be paid when you put the technology to the work it was intended for. This doctrine—probably a contractual element—of ***beneficial use*** is used to trigger payment milestones, as well as to start the warranty and maintenance cycle clocks ticking. The trouble is that it's rare with complex systems to just "flip a switch" and make everything go live.

Implementation more often proceeds in fits and starts. Some functionality exists before the complete system you contracted for is available. Obviously, you don't want warranty clocks ticking for 100 percent of your equipment when only 10 percent of it is in use.

Careful definition of "beneficial use" during contract negotiations will provide leverage during implementation and better value from your equipment.

Sign, Seal, and Deliver!

That's it for the implementation plan. It should pass to the Steering Committee for review before submittal to the project's executive sponsors. If you have involved the project's working committees and built teams to assist with the variety of work discussed, the approval process will be smooth. Once approved, the plan is ready for delivery to all implementation team members.

Manage Documentation

The volume of documentation that can be generated with technology projects is amazing. You've probably already had to buy a new bookshelf just to hold the project planning documents! It's only just begun, though, because documentation is critical in the implementation phase to assure both its proper management and your agencies' ability to use the system over its life cycle.

Six sets or categories of documentation are completed through the implementation phase: **project**, **as-built**, **system**, **equipment**, **procedures**, and **training**.

☐ Project

It probably comes as no surprise that project documentation would be mentioned here first. The implementation plan is the central piece from this phase. Since you can expect it to change during implementation—that's inevitable!—anticipate capturing the details of changes proposed, accepted, or rejected in the audit trail of your plan.

Other important project documentation to capture is all communications with contractors, particularly those involving decisions by one party or the other. Rely on a disciplined process of capturing all paper and electronic communications for the project record. In larger projects, create a formal communications plan and keep a log. Contractual changes can generate a lot of documentation that's important—and probably required by your procurement and legal advisors.

☐ As-built

Depending on your project, as-built documentation includes engineering diagrams, site plans, shelter floor plans, equipment rack layouts, and other depictions of technical aspects of your system. Narrative and other textual information is usually combined with a multitude of diagrams to literally draw pictures of what your system looks like, as built. While much of this information may have been developed during system engineering, its completion during implementation is an important deliverable.

Vendors are typically tasked with completion of as-built documentation. Plan to prepare similar documentation if you take on some responsibility in technical implementation. For example, if you have retained responsibility for providing sites or building facilities that a vendor will use, be sure to include up-to-date site and shelter floor plans in your final system documentation. You will thank yourself later for having done so!

☐ System

System documentation is related to as-built, but focuses on the system's technical aspects more broadly. It may include:

- Logical system diagrams and process flow charts
- Backbone connectivity diagrams
- Disaster recovery procedures
- Maps of sites relative to the involved jurisdictions
- Documentation of predicted and measured radio coverage
- Installation and maintenance standards
- Electrical power service procedures and contingencies
- Location of and procedures for using spare equipment
- Logical mapping of channels and talkgroups
- User radio programming and channel assignments
- Other hardware and software configuration and tuning parameters
- Site permits and frequency licensing information

☐ Equipment

Vendor documentation of all equipment procured and used in the system should be collected, catalogued, and distributed as needed. Quick reference materials either available from the vendor or created by the project team fall into this category. Original equipment specifications, warranties, and installation information can be kept as separate pieces of the broader system documentation.

Portable and mobile radios often arrive *en masse*, are unpacked, inspected, inventoried, and prepared for installation or distribution. Collect user guides from end-user equipment to distribute during training.

☐ Procedures

Both technical and operational procedures are included in implementation documentation. On the technical side, equipment installation and programming procedures are important, as are preventive maintenance schedules and procedures.

SOP development and management is covered in Chapter 12.

Standard operating procedures (SOPs) for both technical and operational use of the technology are an important part of documentation. We will discuss development of operational use of procedures in more detail in Chapter 12.

☐ Training

Training is key to your successful implementation, so be prepared to document *up front* what is to be done and what has been done. Training plans encompassing technician, dispatcher, and field user needs are often outlined in procurement documents and further detailed during implementation. Your training documentation during the implementation phase should also include all materials used by vendors in their contracted training.

Rely on the project working committees for training documentation.

Rely on your User and Technical Committees to create training plans and organize ongoing documentation. Documentation of who received what training, and when, is important for all emergency services skills, including communications.

Use Quality Assurance and Acceptance Tests

The next major step in preparing for implementation is developing acceptance tests. These tests are part of a quality assurance (QA) process that verifies the project is meeting its objectives. They provide a signoff that a vendor has met some term or terms of its contract. The original *Law Enforcement Tech Guide* provides a chapter dealing with developing QA tests that evaluate vendor and product performance. Acceptance testing is the process of assuring quality measures have been met through discrete tests of hardware, software, subsystems, and ultimately the system as a whole.

Make acceptance plans as early vendor deliverables.

Establish creation of acceptance plans as early vendor deliverables. While most testing and all acceptance is your responsibility, of course, you may be able to adapt standard test plans that your vendor provides.

Adapt canned test plans to your project.

Evaluate the standard plan, and then take the time to develop these plans further by removing any elements unrelated to your implementation. Add others central to your functional specifications. Through an iterative effort, you will be able to establish an acceptance test plan that meets your needs and provides project quality assurance. A good test plan adequately and accurately tests the technology as proposed by the vendor and as contracted for.

In large projects, it makes sense to refine acceptance tests through multiple phases. For example, an early phase of a wireless local area network (WLAN) implementation may target the central facilities of the involved agencies, while leaving outlying stations for later. Development and use of the acceptance plan in the first phase will likely lead to changes for subsequent phases. If you choose that option, make note of it in your implementation plan. Remember: the more money involved, the more is riding on the acceptance process, and the more planning that is needed.

Testing

In conducting the acceptance tests, user involvement is important to successful implementation—and a successful project. Your acceptance team will probably be composed of some project participants who have been involved from the beginning. It should include members of the User and Technical Committees who will be responsible for verifying that the project's requirements are met.

As discussed in the original *Law Enforcement Tech Guide*, there are three common benchmarks for testing technology: **functionality**, **reliability**, and **performance**. Systems implemented for communications interoperability that make use of radio technology also usually include special performance testing for **coverage**.

☐ Functional Testing

Staged testing helps minimize costs for large systems.

Functional tests are designed to ensure that the equipment and subsystems work as advertised and proposed. They may take place when the system is staged, after it is installed, or both. Large system implementations commonly require that the equipment vendor *stage*, or assemble, equipment at the vendor's facilities where it is then tested for functionality. This provides some integrated testing of the vendor's offerings. Staged testing helps minimize costs for large systems by providing a controlled environment where subsystems are immediately accessible—as opposed to being on a mountaintop somewhere!

Final functional testing takes place once equipment is installed. The vendor repeats the tests performed in staging and conducts additional tests arising from the equipment's integration into its physical location and other systems. For example, radio systems are very much dependent on their antenna subsystems. Functionality of some aspects of the radios can only be adequately tested once the equipment is in place, antenna systems installed in their final locations, and other subsystems integrated.

☐ Reliability Testing

Reliability testing typically requires some sort of simulation. As discussed in the original *Law Enforcement Tech Guide*, software can be tested for reliability through use of special applications designed for this very purpose. With hardware, including radio equipment, time is the only reliable reliability test.

Systems, as we've discussed them here, are a complex of software, hardware, and human aspects. The software and hardware parts form their own subsystems that can be tested by simulating "faults" between components. For example, a shared mobile data system with a single mobile server, but multiple agency CAD and RMS connections, could be tested for reliability as the connections to the agencies' information systems are broken. This would show how other parts of the system perform under less-than-ideal conditions.

Similarly, radio components may be tested as they lose backbone connections between sites, power, or even antenna system connections. Advanced systems use active networking monitoring techniques and devices for detecting faults. Conduct functional testing of these subsystems while forcing system faults to conduct reliability testing elsewhere.

Each testing step toward implementation constitutes further integration testing.

☐ Performance Testing

The third stage of acceptance testing involves getting right down to measuring how well the technology meets the operational requirements driving its procurement. Subsystems, such as backbone networks connecting radio sites and other fixed facilities, can be *incrementally* tested for performance. On the other hand, *final* performance testing requires that all subsystems be installed, configured, optimized, and integrated.

Performance testing of potentially wide-ranging, multiagency systems for communications interoperability can be challenging. Consider using limited exercises once equipment is installed and training conducted. Appropriately timed, exercises can serve as near-real performance tests leading to acceptance. Full-scale exercises can be the next best (worst?) thing to an actual emergency to stress-test communications systems.

☐ Coverage Testing

A type of performance testing peculiar to radio systems is coverage testing. Radio coverage testing involves field measurements of signal strength and a healthy dose of science mixed with probability statistics. Without getting into the heavy details,[55] radio coverage varies greatly based on distance and intervening obstacles between the transmitter and receiver. Obstacles can be everything from buildings to the human body. Coverage also varies over time at any given spot. Radio system designers work to account for these variations in predicting coverage.

It's not a matter of simply driving around saying, "Can you hear me now?"

Typically, public safety agencies specify coverage requirement as a percentage of a geographic area under certain conditions and to a certain level of audio quality, for example: 95 percent coverage of the city is required for a Delivered Audio Quality (DAQ) of 3.4 with portable radios carried outdoors at the hip, for both transmit and receive.

Obviously, coverage testing during implementation to verify this is going to take some technology, statistics, and work. It's not a matter of simply driving around saying, "Can you hear me now?"

If your project requires it, coverage testing is not something to be taken lightly! It's one of those areas of implementing technology for which you should hire qualified assistance if you don't have the expertise internally.

55. The accepted standards for coverage testing are defined in the Telecommunications Industry Association (TIA) Telecommunications Systems Bulletin TSB-88, "Wireless Communications Systems, Performance in Noise- and Interference-Limited Situations, Recommended Methods for Technology-Independent Modeling, Simulation, and Verification." Note that this is not a formal standard, but an accepted technical methodology. For more information, see www.tiaonline.org.

Sample Functional Acceptance Tests

While this incremental process of testing should be understandable, there's nothing like examples to make them real. Figure 10-2 shows a few of the functional acceptance test procedures used by the City of Mesa (Arizona) in implementing its trunked radio system. Many more in each category were used, as were yet more categories of procedures. Each procedure was accompanied with the required setup process to assure that resources needed for the test were prepared. This plan was provided in draft by the vendor and worked out in detail with the agency through implementation planning.

As each test was successfully completed, team representatives from the agency and the vendor signed off on it with any additional notes memorializing the test.

Figure 10-2: Excerpts from City of Mesa (Arizona) Acceptance Test Plan

Site Trunking		
Feature	Description	Test
Site Trunking Talkgroup Call	When a site goes into site trunking, radios with talkgroup call capability will be able to communicate with other members of the same talkgroup at that same site. Members of the same talkgroup at other sites will not be able to monitor those conversations.	**Step 1.** Place Site 1 into the site trunking mode. **Step 2.** Initiate a talkgroup call with RADIO-1 on Test TG 1 at Site 1. **Step 3.** Observe that only RADIO-2 will be able to monitor and respond to the call. **Step 4.** Initiate a talkgroup call with RADIO-3 on Test TG 1 at Site 2. **Step 5.** Observe that only RADIO-4 will be able to monitor and respond to the call.
Call Alert	Call alert is a tone page that allows a user to selectively alert another radio unit. When a site is in site trunking, Radios at the site will only be able to call alert other radios at the same site. The initiating radio will receive notification from the trunked system as to whether or not the page was received by the target radio.	**Step 1.** Place Site 1 into the site trunking mode. **Step 2.** Using RADIO-1, press the alert button. **Step 3.** Enter the Unit ID of RADIO-2 with the keypad, or scroll to the location where this ID is stored. **Step 4.** Press the PTT to initiate the call alert. **Step 5.** Verify that RADIO-2 received the call alert. **Step 6.** Exit the call alert mode and return to normal talkgroup mode.

Figure 10-2: Excerpts from City of Mesa (Arizona) Acceptance Test Plan *(con't)*

Wide Area Trunking		
Feature	**Description**	**Test**
Talkgroup Call	Radios with talkgroup call capability will be able to communicate with other members of the same talkgroup. This provides the effect of a private channel down to the talkgroup level. This test will demonstrate that a talkgroup transmission initiated by a radio user will only be heard by system users who have the same talkgroup selected. As with other types of calls, talkgroup calls can take place from anywhere in the system.	**Step 1.** Initiate a wide area call with RADIO-1 in Test TG 1. **Step 2.** Observe that only RADIO-2 will be able to monitor and respond to the call. **Step 3.** Initiate a wide area call with RADIO-3 in Test TG 2. **Step 4.** Observe that only RADIO-4 will be able to monitor and respond to the call.
Secure Operations	Digital encryption is used to scramble a transmission so only properly equipped radios can monitor the conversation. A "key" is used to encrypt the transmit audio. Only radios with the same "key" can decrypt the audio and listen to it.	**Step 1.** Initiate a secure wide area call with RADIO-1 on Test TG 1. Keep this call in progress until instructed to end the call. **Step 2.** Observe that RADIO-2 will be able to monitor and respond to the call. **Step 3.** Observe that RADIO-3 does not receive the call. **Step 4.** Observe that RADIO-4 will also receive the call even with the secure switch set to the nonsecure mode of operation. **Step 5.** End the call from RADIO-1. **Step 6.** For radios equipped with dual algorithm encryption modules, select a talkgroup using the second algorithm and repeat Steps 1-5.
Call Alert	Call alert is a tone page that allows a user to selectively alert another radio unit. The initiating radio will receive notification from the trunked system as to whether or not the page was received by the target radio. Units receiving a call alert will sound an alert tone. As with other types of calls, call alerts can take place from anywhere in the system.	**Step 1.** Using RADIO-1, press the page button. **Step 2.** Enter the unit ID of RADIO-2 with the keypad, or scroll to the location where this ID is stored. **Step 3.** Press the PTT to initiate the call alert. Verify that the RADIO-1 user receives audible indication that the call alert was sent. **Step 4.** Verify that RADIO-2 user receives an audible indication of an incoming call alert that was sent but RADIO-3 does not. **Step 5.** Verify that RADIO-1 gets an audible indication that the call alert was successfully received at the target radio. **Step 6.** Turn off RADIO-2. Send a call alert from RADIO-1 to RADIO-2. **Step 7.** Verify that the RADIO-1 user receives audible indication that the call alert was sent. **Step 8.** Verify that RADIO-1 receives an indication that the call alert was not successfully received at the target radio.

Figure 10-2: Excerpts from City of Mesa (Arizona) Acceptance Test Plan *(con't)*

Console		
Feature	**Description**	**Test**
Talkgroup Selection and Call	Dispatchers with talkgroup call capability will be able to communicate with other members of the same talkgroup. This provides the effect of an assigned channel down to the talkgroup level. When a talkgroup call is initiated from a subscriber unit, the call is indicated on each dispatch operator position that has a channel control resource associated with the unit's channel/talkgroup.	**Step 1.** Initiate a wide area call from any operator position on Test TG 1. **Step 2.** Observe that RADIO-1 and RADIO-3 will be able to monitor the call. De-key the console and have either radio respond to the call. **Step 3.** Observe that all consoles with Test TG 1 can monitor both sides of the conversation. **Step 4.** Initiate a wide area call from any operator position on Test TG 2. **Step 5.** Observe that RADIO-2 and RADIO-4 will be able to monitor the call. De-key the console and have either radio respond to the call. **Step 6.** Observe that all consoles with Test TG 2 can monitor both sides of the conversation.
Talkgroup Patch	Talkgroup patch allows a dispatcher to merge several talkgroups together on one voice channel to participate in a single conversation. This can be used for situations involving two or more channels or talkgroups that need to communicate with each other. Using the patch feature, the console operator can talk and listen to all of the selected talkgroups grouped; in addition, the members of the individual talkgroups can also talk or listen to members of other talkgroups. Patched talkgroups can communicate with the console dispatcher and other members of different talkgroups because of the "supergroup" nature of the patch feature.	**Step 1.** Select an operator position for testing which contains Test TG 1 and Test TG 2. **Step 2.** At the desired operator position, select the patch tab in the patch window. **Step 3.** Click the button on the patch that allows an operator to set up and edit a patch (note patch window turns blue). **Step 4.** Add Test TG 1 and Test TG 2 to the patch by selecting each resource tile. **Step 5.** Once the talkgroups are added, click the patch setup button again to complete the patch setup. **Step 6.** Initiate several talkgroup calls between radios. **Step 7.** Observe that all radios are able to communicate with one another. Also via subsystem viewer screen, observe that only one station is assigned at each of the two sites. **Step 8.** Initiate a call from the operator position using the patch transmit button and observe that all radios are able to receive the call and only one station is assigned at each of the two sites. **Step 9.** Remove Test TG 1 and Test TG 2 from the patch.

Figure 10-2: Excerpts from City of Mesa (Arizona) Acceptance Test Plan *(con't)*

Report Generation		
Feature	**Description**	**Test**
Historical Reports	Performance reports can be created automatically for dynamic statistical information about the air traffic activity on the system. These reports provide assistance with system management, resource planning, usage allocation, and monitoring. All reports are preformatted and summarize air traffic activity for a configured time span.	**Step 1.** From the application launcher, select a subsystem. **Step 2.** From that subsystem's menu, choose subsystem historical reports. **Step 3.** From the historical reports window that opens, select a report. **Step 4.** Using the left mouse button, click on the view button. **Step 5.** Observe a window opens, allowing a user to enter report parameters. **Step 6.** Enter all desired data for the report and generate report. **Step 7.** Observe a window appears showing the requested report. **Step 8.** Close the report window. **Step 9.** Run the following reports during testing: Talkgroup at Subsystem Summary; Radio User at Subsystem Summary; Site Summary.
System Reliability		
Simulcast Essential Site Operation	This test verifies the essential site operation within a simulcast system. An essential simulcast remote site is one that must have at least one control channel and one traffic channel for the simulcast subsystem to remain in trunking mode. If all control channels or all traffic channels have experienced faults at an essential simulcast remote site, then the entire simulcast subsystem is put into failsoft mode to ensure communication can continue in the area covered by the essential simulcast remote site. When all of the wide area failsoft channels at an essential simulcast remote site have experienced faults, the essential simulcast remote site is malfunctioned.	**Step 1.** Power down one of the control channel capable stations at the non-essential site and note that configuration software shows the channel is disabled at all the other sites. **Step 2.** Repeat Step 1 for each of the other control channel capable stations or until 50% or more of the stations have been malfunctioned. **Step 3.** Verify that configuration software shows that the disabled channels have been enabled at all other sites in the simulcast subsystem and that RADIO- 1 can communicate with RADIO-3. **Step 4.** Repower all of the control channel capable stations at the non-essential site. **Step 5.** Power down all of the control channel capable stations at the essential site. **Step 6.** Verify that the simulcast subsystem is now in the failsoft mode. **Step 7.** Re-power all of the control channel capable stations at the essential site and verify the simulcast subsystem is back in wide-area trunking.
Base Station Identification	This test verifies that the repeaters programmed for base station identification at every site broadcasts the FCC identifier every 30 minutes. To accomplish this, a service monitor will be set up to monitor the identification channel of a random site and note that the Morse code is heard.	**Step 1.** Choose one site to test for base station identification. **Step 2.** Set up the service monitor to receive the frequency of the identification channel for the particular site. **Step 3.** Monitor the service monitor until the system ID is broadcast.

Create Standard Operating Procedures and Train

More likely than not, your agencies will have a few existing policies and procedures that shaped earlier functional specifications and now have to be incorporated with the new system. We earlier recommended forming the policies/procedures team prior to procurement to start collecting and melding policies and procedures between agencies. If the team has been productive, you should have a core set of standard operating procedures (SOPs) around which training can be developed.

We recognize that developing operational policies and procedures proceeds more easily when users have real technology up and running. It's a living process that will hopefully have its start in your system design, procurement, and implementation, and then mature as the system moves to full operation.

In Chapter 5 we introduced you to the SAFECOM template suite that you can use to develop memorandums of understanding and other formal agreement documents. The SAFECOM suite also includes several templates for developing interoperability SOPs. We delve more deeply into SOPs, including the SAFECOM templates,[56] in Chapter 12, **Develop Policies and Procedures**, in recognition of that ongoing process.

Your next step is to develop training programs using your own internal operational expertise as to how the system should be used. In large projects, training development and execution is contracted out because it can be a huge undertaking. Again, look for operational expertise, not necessarily technical, in developing training for end users.

Initial training may be contracted out.

Vendor training on the equipment and system basics is valuable, particularly for your agencies' trainers who will then go on to incorporate information about the technology into their own training programs. Don't rely on the equipment or system vendors to conduct the bulk of training. They typically have good technician programs, but limited expertise on how the technology is best put to work by end users.

If the system will rely on dispatchers to activate resources or use the technology, include special training for all dispatch agencies involved. Consider building internal expertise within dispatch agencies involved in your project through "train the trainer" courses contracted with either a commercial training company or through peer agencies elsewhere in the country that have been successful with similar projects.

Use "train the trainer" courses to build self-sustaining expertise.

56. These are available at www.safecomprogram.gov/oecguidancedocuments/webpages/ts.aspx.

Traditional classroom training is of limited use when it comes to interagency communications. Theory and diagrams don't do enough to instill communications skills needed by first responders. Tabletop exercises are useful to introduce new systems, work out procedural bugs, and establish an understanding of the sequence of tasks in using the new capabilities. In short order, though, you'll need to move to a realistic environment.

Train in the context of how the technology will actually be used.

Train for use of your new system in the context that it will actually be used. Put radios, laptops, and keyboards in responders' hands, show them how the capabilities are used, and then have them practice until their skills are developed to an acceptable standard. Assuming capabilities will be placed in the hands of all responders, training will need to be further incorporated into their basic training programs, on-the-job training, and exercises so the skills are gained by new recruits and refreshed among old-timers alike.

We'll have more to say about training methods in the next chapter on maintaining your system and processes.

With an implementation plan in place, acceptance tests lined out, and training of end users and support personnel planned, your project is well-positioned for a successful implementation.

An Example

The process of moving from needs analysis through implementation has been described in detail. To finish up this chapter, which is intended to guide you to an operational system, let's use an example to make the implementation process a bit more tangible.

The example is a hypothetical case used to capture a composite mix of activities, but based on very real initiatives going on around the country. It captures the mixture of responsibilities across the project team and your vendor showing how they need to be timed and communications shared.

Three small cities and a county have joined in an interoperability initiative to improve communications interoperability. Alphaville, Bravotown, and Charlieport are independent municipalities in Delta River County.

Delta River County: As-is

- **Alphaville** has a conventional voice radio system using separate repeated channels[57] in the UHF band for police, fire, and EMS dispatch. APD and AFD each have direct portable-to-portable channels for their internal tactical needs. Both have two state-designated mutual aid channels installed in their portable and mobile radios for talking directly to other UHF users, but the channels are only useful on-scene since they aren't repeated. APD uses mobile data computers in patrol cars to receive routine dispatches; run wants, warrants, and motor vehicle checks; and for some car-to-car messaging.
- **Bravotown** shares a conventional voice radio system on VHF-high band with Delta River County. Dispatch of the county sheriff, volunteer fire departments, BPD, and BFD is all handled by a consolidated dispatch center over the same set of four repeaters spread around the county, although there are separate law enforcement and fire channels. The repeaters are linked together so they simultaneously transmit the best received signal on the channel anywhere in the county.[58] The volunteer fire departments have a shared tactical channel between them for unit-to-unit communications, as do each of the law enforcement agencies for their intra-agency use. All of the VHF-high band users have five state-designated mutual aid channels installed in their mobile and portable radios that are useful for direct communications. EMS services are provided by fire department quick response units and a commercial ambulance service, which are all dispatched on the same fire channel.
- **Charlieport** has a relatively new 800 MHz trunked radio system[59] for voice communications. All municipal users are on the system. Portable and mobile radios are also programmed with five state-designated mutual aid channels, which also happen to be nationally standardized. These are typically used to communicate unit-to-unit with state police and highway maintenance responders that use a similar statewide system. CPD and CFD use a common mobile computer system with wireless services provided by a commercial carrier.

57. A *repeater* is a radio typically permanently fixed with an antenna well situated on a tower or other high spot in the jurisdiction that receives radio communications on one frequency and retransmits them on another frequency within the same band. See Chapter 16, pages 281–282, for more detail and a diagram.

58. This is known as a *simulcast* system with receiver voting. For practical purposes, the system can be thought of as a single repeater with the wide, composite coverage provided by all the separate sites. The effect is a single channel that covers a wide expanse, which can be good at times and bad at others, depending on whether distant communications are needed or are only interfering with more pressing, shorter-range ones.

59. A *trunked radio system* uses repeaters, too, but computers in the radios and at the heart of the system automatically assign their use to individual conversations between groups of users, or *talk groups*. This makes channels defined functionally, rather than defined electronically or geographically.

While this is a hypothetical scenario, it is very realistic and exists in similar form all around the country. In our example, all these agencies have joined in a countywide initiative to improve interagency communications for first responders. Let's take a look at the system of systems they chose and what's involved in implementing it.

Delta River County: To-be

Through a needs analysis and conceptual design, the agencies decided to use a combination of approaches to improve their interoperability. The Steering Committee concluded early on that both voice and data communications were important. Jointly, the agencies first issued an Invitation for Bids (IFB) and hired a systems integrator, then followed up with a request for proposal (RFP) to procure the technology. Functional specifications were created around their requirements and the conceptual design. They called for the following:

- A cache of 16 VHF-high band portable radios programmed for all the county's channels and five state mutual aid channels in the band. These will be used for a command net during extended interagency incidents.
- One new channel added to the county's conventional system for interagency use and one new site in Charlieport to improve the system's coverage in the denser downtown area.
- A fixed gateway device in Charlieport capable of interconnecting an existing CPD/CFD command talk group to the new county interagency repeated channel and Alphaville direct command channels. The gateway will be controlled by Charlieport central dispatch.
- A mobile gateway device to be housed, maintained, and fielded by AFD. It will be used to interconnect Charlieport mutual aid responders outside of the range of their system to other responders using direct 800 MHz, county VHF-high band, and Alphaville UHF mutual aid channels. Similarly, it will bring AFD and APD direct channels into interconnected groups outside the range of the Alphaville primary system. In effect, this device will serve as a mobile crossband repeater for linking channels around an incident site.

- An intersystem message switch for connecting the Alphaville and Charlieport mobile data systems together to allow car-to-car and dispatch-to-dispatch messaging. The system's primary use for interagency communications will be for messaging between dispatch centers, incident command posts, emergency operations centers (EOC), and evacuation centers. Fixed terminal access to the Charlieport system will be established in the Delta River Central Dispatch and EOC.

This initiative uses a combination of approaches to the technical side of interoperability described in the SAFECOM *Interoperability Continuum*. In use, there will be swapping of radios from the cache to add capabilities, gateways to patch together existing systems, shared channels designated specifically for interagency communications, and a shared system by some responders. It doesn't, however, replace all existing radio systems with a single, shared one. Doing so may be a future possibility as Delta River County's needs expand and agencies become more accustomed to requesting and providing mutual aid outside the coverage of their individual systems, but for now this approach serves their interoperability needs.

Delta River County: The Implementation

With the scenario laid out, let's take a look at what will be required for implementation.

Through the RFP, the partners made multiple awards. The first went to a nearby radio communications service shop for delivery of the cache radios, programming, and packaging in a deployable case. The second went to a large radio systems vendor for most of the other work, except for the mobile data system interconnect, which went to a third company. Training of users and technicians was included as a task under all three contracts.

Following the original *Law Enforcement Tech Guide*, the Delta River project manager pulled together a draft implementation plan from materials in the original project plan and new contracts. He had the systems integrator draft an acceptance plan in cooperation with the other contractors while the implementation plan was being put together.

Several teams were assembled to work through implementation. Most of the members of the procurement team that guided the IFB and RFP efforts moved on to the acceptance team, which was responsible for conducting the actual tests to assure that the system performed as intended.

Initiate changes to policies, procedures, and agreements early on.

A **policies/procedures team** was brought together from key members of the User Committee. It was charged with again reviewing all the agencies' relevant policies, SOPs, and mutual aid agreements that went into a business process baseline report. The team was further charged with drafting the new policies and procedures needed for the use of their new capabilities. The team used the SAFECOM template suite during this process.

The earlier needs analysis process had turned up some procedural holes in the countywide emergency operations plan, particularly as it defined the command structure for interagency response. While the Incident Command System (ICS) was commonly *expected* to be used, few agencies in the county regularly used it.

Integrate expected changes to incident response into the new system of systems.

With funding being increasingly tied to use of the National Interagency Management System (NIMS), the policies/procedures team found this was a good time to put some definition to how agencies in the county would use NIMS-based ICS for interagency operations. Working through their agencies and the project User Committee, the team came up with new draft procedures describing interagency command processes and worked them through the Steering Committee for approval. The project's executive sponsors carried the new operating procedures and their communications counterparts through the Local Emergency Planning Committee (LEPC) required by state and federal legislation.

Use outside resources for help managing project construction.

Elsewhere in the project, a **construction team** was assembled with the Steering Committee's approval to guide the development of the new Charlieport radio site. The team consisted of the Charlieport facilities director, a county zoning officer, a CFD captain who served on the city's earlier steering committee for its 800 MHz system, and a CPD technical services manager responsible for daily operations of the system, who also chaired the initiative's Technical Committee. The team's charge was to select an appropriate site, with the guidance and eventual concurrence of the system vendor, that provided adequate coverage, was affordable and acceptable, and ideally was on city- or county-owned property.

The **acceptance team** built a series of tests for each of the system's technology components that would lead them to acceptance of the pieces and eventually the system as a whole. A previously planned LEPC tabletop exercise provided a good venue for testing the radio cache when it was delivered. Tests turned up needed programming changes and suggestions for additional battery packs, which was outside the contract, but was negotiated for through a change order with the vendor after the Steering Committee approved doing so.

Acceptance testing of the fixed and mobile gateways proceeded through three steps: functional, reliability, and performance testing. Functional testing was performed by the team with additional help from members of the Technical Committee. It followed a script calling for separate radios from each of the agencies to be brought to Charlieport, activation of the gateway, and then testing transmissions sent back and forth. The mobile gateway was similarly tested in Alphaville.

Functional, reliability, and performance tests were conducted.

Reliability testing of the gateways was conducted over the period of a month with daily activations of the devices and weekly testing of actual transmissions between agencies. Performance QA tests were conducted during all the functional and reliability tests. They consisted of minimum setup and breakdown times for the devices themselves, as well as individual connections between channels. Audio quality and induced delay tests were also performed to see if the gateways materially affected communications. Most important, functional tests allowed the partners to look for negative tests the gateways had on their existing systems, such as connecting repeated systems in a loop.

Reliability testing takes time.

The intersystem message switch between Alphaville and Charlieport mobile data systems was similarly tested on all three levels. The acceptance team contacted agency references provided by the radio system vendor and adapted their test plans from a similar implementation. They also made use of sample language provided in the original *Law Enforcement Tech Guide*, further customized to include tests across both jurisdictions' dispatch points, the new EOC installations, and directly between responders.

Adapt existing tests from other agencies and sources.

Delta River County: Acceptance

Implementation proceeded smoothly. Each of the vendors had good experience with similar projects and worked well with the project manager to build a realistic schedule before starting work, then made adjustments through the Steering Committee concurrence to both lengthen and shorten phases as it proceeded. Only a couple of contractual milestones were at risk of being missed. The project manager, vendor's managers, and the acceptance team sat down and adjusted work in other parts of the schedule to rebalance the timeline. One deadline was breached, but all parties agreed that it was due to delays in frequency licensing, which was Delta River's responsibility, and no penalty clause was invoked.

Adjust the schedule by shuffling work internally, if possible.

Training was designed by the policies/procedures team from materials provided by the vendors under contract. The vendors provided early training to key dispatch, technical, and field supervisors who would be expected to understand parts of the system more thoroughly to conduct further staff training. This "train the trainer" approach is commonly used to capture as much knowledge and technique as possible from the vendors in building a cadre of future instructors.

Anticipate that training will be a perpetual process.

Further training continued as various parts of the system were put into place. It was timed so that, if the schedule went as planned, there would be no more than 6 weeks between hands-on training and final acceptance.

Final acceptance was contingent on a full-scale exercise that was planned and scheduled by the acceptance team through the LEPC starting early in the project. The exercise brought out police, fire, EMS, and emergency management personnel from across the county in a tornado scenario. Since the county had regularly used such scenarios for emergency planning in the past, it provided a good opportunity to stress-test the new system of systems—complete through all technology elements, policies and procedures, and training.

Use exercises for performance testing.

The exercise pointed out needed adjustments in procedures for activation of the fixed gateway and coordination of its use with technicians deploying the mobile gateway in order to reduce any future interference between the two. These adjustments were entirely the responsibility of the project team, so didn't affect final acceptance and payment to the vendor. A error in the mobile data interconnect configuration that prevented direct messaging between the Charlieport and Alphaville EOCs was identified as out of specifications, though, and that vendor was able to quickly fix the problem.

Use successful final tests to congratulate the team and set the stage for future interagency collaboration.

A small ceremony and press conference was held the morning following the exercise by the project's executive sponsors. They used media attention to the exercise—and successful testing—to announce that the project had been successfully completed. Separately, they met with the vendors' representatives and formally accepted all the remaining contractual elements, releasing the final 10 percent of payment.

The system of systems is the functional collection of people, technology, and business processes.

The project was completed on time and budget (of course!). Training was a key part of its success, starting with the tabletop exercises for functional testing, to traditional "train the trainer" methods, and on to training in the real context of how the system will be used. This focus on training means the collection of technologies, policies, procedures, and people will work as a single system.

CHAPTER 11

Transition to Long-term Governance

What: Long-term governance refers to the ongoing work to keep technology and organizational processes working toward interoperability goals over the life cycle of the system.

Why: All systems, natural and manmade, can experience entropy, deteriorating over time if left unattended. Communications interoperability isn't a one-shot proposition.

Who: A revised governance structure, involving many of the project's participants, is needed to maintain the system of systems over its life cycle. The Steering Committee bears the responsibility of creating the ongoing structure before dissolving the project team.

When: Immediately after implementation, the project has to be closed out and the maintenance phase begun.

Chapters 18 and 19 of the original *Law Enforcement Tech Guide* cover *project closeout, maintenance,* and *grant management for technology projects in general.*

If you have followed this Guide in carrying out a communications interoperability project, congratulations are in order. Following implementation of the technology and processes to put it to work, there is cause for celebration as your agencies move into the subsequent and long-term phase of systems maintenance. There are a few final project details to attend to, but we're going to suggest you do this very thing soon: celebrate!

A System of Systems

We've used the term "system of systems" throughout this Guide. Your communications interoperability system, for better or worse, richer or poorer, is the collection of policies, procedures, and technologies, as well as training and exercises that tie it all together. As we've said, all systems have geographic, technical, and functional boundaries. They also have administrative boundaries where jurisdictions participating in your system of systems have to work with "outsiders."

SAFECOM 20-year Vision

Established 2003

There is an integrated system-of-systems, in regular use, that allows public safety personnel to communicate (voice, data, and video) with whom they need on demand, in real time, as authorized.[60]

All communications systems have boundaries.

Over time, successful communications interoperability systems have a way of melding with neighbors at the borders. If public safety agencies are able to create an integrated system of systems, nationally, it will be a complex of different technologies *and* procedures that meet the needs of agencies rural and urban, large and small, paid and volunteer. It will support all who have to respond to emergencies that don't respect geographic, technical, functional, and administrative boundaries.

Systems—in all their animate and inanimate dimensions—have to be maintained over time. Communications interoperability systems are no exception and will, indeed, otherwise deteriorate rapidly due to their dependence on the proper functioning of so many pieces.

In addition to the technology that you've just implemented, this life cycle maintenance encompasses the governance and management structures that drive the system, the policies and procedures that define it for all practical purposes, and the training and exercises that make it real.

60. U.S. Government Accountability Office, Homeland Security: *Federal Leadership and Intergovernmental Cooperation Required to Achieve First Responder Interoperable Communications*, GAO-04-740, Washington, D.C.: July 2004, p. 54. See also *Enhancing Communications Interoperability: General Guidance and Recommendations for Interoperability-related Governance*, SAFECOM, 2006. www.safecomprogram.gov/library/Lists/Library/Attachments/108/GeneralGovernanceRecommendationsDHSapproved.pdf. See also *Establishing Governance to Achieve Statewide Communications Interoperability*, 2008. www.safecomprogram.gov/library/Lists/Library/Attachments/241/Establishing_Governance_to_Achieve_Statewide%20Communications%20Interoperability.pdf.

Life cycle planning is a continuous cycle of improvement made possible by the relationships and skills of people. Planning, coordination, and cooperation keep this cycle in motion so technology will work in a reliable, efficient, and effective way to meet the needs of current and future users of the expensive and complex communications and information sharing systems.

> *"System life cycle planning is needed to ensure long-term sustainability of communications systems and infrastructure." (SAFECOM 2011)*[61]

A life cycle planning requirement is one of the key ways that SAFECOM's grant guidance has changed. The Department of Homeland Security urges agencies applying for grants to engage in life cycle planning. Many federal granting agencies now require that applicants submit a system life cycle plan with their grant applications.[62]

Project Closeout

Before moving on to the long-term, recurring processes of maintenance, we have a few loose ends with the project to wrap up. The project will reach completion through the following steps.

Hold a Transition Meeting

Hold a meeting to hand over the keys.

As mentioned in Chapter 10, complex systems are managed by vendors through installation. At some point, often in a series of steps, system management is handed over for long-term maintenance. You may have chosen to have one or more of your vendors stay on to maintain portions of the technology over time, but typically there are still configuration and monitoring tasks, at least, to transition.

A final transition meeting is useful to get everyone in one room to hand over the keys to the technological components of your new system. Proceed by involving project management and vendor staff, as well as the technicians and all stakeholders who will be charged with maintaining the hardware, software, and other physical components of the system. Follow the transition meeting with a larger, open meeting for broad attendance.

61. U.S. Department of Homeland Security, Office of Emergency Communications, Emergency Communications System Life Cycle Planning Guide, August 2011. See www.safecomprogram.gov/library/lists/library/DispForm.aspx?ID=324.

62. FY2011 SAFECOM Guidance on Emergency Communications Grants continues to provide guidance on eligible emergency communications activities and equipment. See .www.safecomprogram.gov/SiteCollectionDocuments/FY_2011_SAFECOM_Guidance_121510.pdf.

Conduct an Open Review Meeting

Too often, projects wind down or drag on without a real end point. This has an unfortunate effect on project participants who, naturally, need to see a positive endpoint that signals success.

Recognizing that there are processes that will continue on for weeks and months to come, find a natural breakpoint to hold an open review meeting. Conduct a review where executive sponsors, the Steering Committee, and the rest of the project team can sit down to examine the project from start to finish. Honestly evaluate how well the project's objectives were met and how the process to achieve them varied from original expectations. SEARCH developed a project management resource toolkit that contains a project assessment checklist. Based on the SAFECOM self-assessment process, the checklist provides a simple way to evaluate public safety projects.[63] Ask the simple question of what participants would do differently if they were to undertake the same project again.

Use the opportunity to publicly declare success.

Use the open review meeting to celebrate the successful completion of your project. The completion of the meeting is a great time for the executive sponsors to issue press releases and otherwise publicly announce the project's completion and its success. With large projects, use a public forum afterward to present the project, problems faced, and hurdles overcome.

Carefully document all discussions, as they will be useful in your last job as project manager: the final report.

Write a Final Report

Contribute lessons learned in your final report for the benefit of others.

For the sake of those who follow, write a final project report. It may be a requirement if the project was grant-funded, but it should be considered necessary for every project.

The report documents the final project timeline and costs. It also documents how the project's objectives were met and what performance measures were used to assure quality. A final budget and cost accounting is critical for both understanding and justifying costs. Your past work to keep the project and implementation plans up-to-date will simplify this task!

63. The Project Planning Resource Toolkit is based upon work supported by the U.S. Department of Homeland Security under Grant Award number 2010-PD-124-000001. The toolkit is available online at www.search.org/products/.

The report will be of most use to future readers from your agencies and perhaps others if it includes a succinct statement of lessons learned during the project. These are likely to be organizational, managerial, and operational lessons as much as they are to be technical ones.

In our work with jurisdictions across the country that are striving to improve communications interoperability, we find the most meaningful lessons coming from other agencies that have been down similar paths. Contribute your lessons learned as a special section of your final report.

☐ Get Internal Acceptance

Wrap up the project by delivering the final report first to the Steering Committee and then to the executive sponsors for their review, changes, and eventual approval. Use a simple signing ceremony to officially close the project.

A cardinal principle of Total Quality escapes too many managers: You cannot continuously improve interdependent systems and processes until you progressively perfect interdependent, interpersonal relationships.
—*Stephen Covey*

Govern and Manage

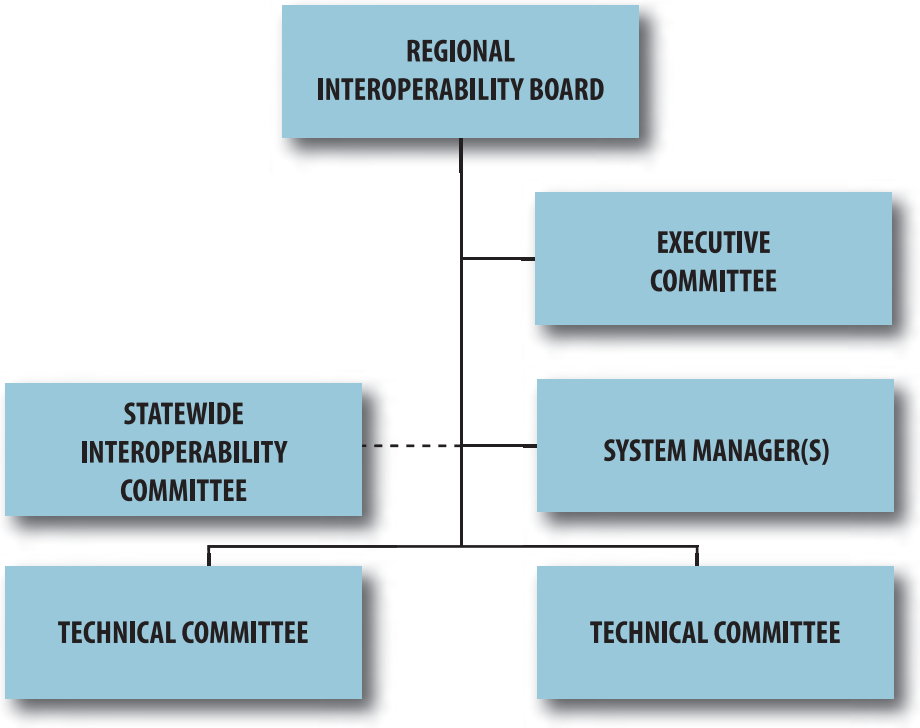
We should be so fortunate that signatures on the final report signal the achievement of communications interoperability. The reality is that the project end marks the beginning of a process of ongoing governance and management. It's a process necessary for continued interoperability and continuous improvements that will go on as long as agencies need to communicate with one another.

The project Steering Committee should create an ongoing governance and management structure to assume the helm upon its own dissolution.

Build Long-term Governance Structures

Long-term and project governance structures vary in at least a couple of ways. Obviously for starters, long-term structures are intended to remain in effect indefinitely, which leads to a different dynamic between participants. The need for executive sponsorship separate from steering has disappeared. While processes always need champions, the most effective champions for ongoing governance are those who can participate in its regular, if less frequent, deliberative meetings. Agency executives who are able and willing to actively participate will lend strength to ongoing governance and management, however.

Figure 11-1: Sample Ongoing Governance Structure



Ongoing processes need champions, but not executive sponsors.

In addition, many representatives who would insist on being part of the Steering Committee will now be comfortable stepping back from regular meetings and delegating ongoing oversight to joint representatives. This may be a process that takes a while, but will occur over time.

☐ Create the Board or Council

The ongoing governance structure doesn't need to be significantly different from that used for the project. Some of the titles change and reporting responsibilities vary a bit, but otherwise there can be a smooth transition from the project to maintenance phases. See Figure 11-1 for a sample governance structure.

Your structure will vary, as did your project governance, based on the scope of your initiative. Whether the project is large or small, ongoing oversight can be provided by a similar, but smaller group. Large initiatives for widely shared systems face difficult choices between models, such as creating independent governmental or

quasigovernmental organizations or partnering with private companies. Regional projects, on the other hand, typically act as consortia of independent jurisdictions operating under mutual agreement.

Adapt your project governance structure for ongoing needs.

A typical long-term governance structure for a moderately-sized initiative, costing from a few hundred thousand to several million dollars, needs no more than a central board, User and Technical Committees, and one or more hired or designated managers.

Seriously consider limiting the size of the board. Any body that has more than 10 members needs an executive committee of fewer people to get work done between meetings. All participating jurisdictions can and should be represented, although they don't necessarily need a seat on the board.

☐ Partner with the Statewide Interoperability Committee

States have created statewide interoperability committees or councils to more broadly guide efforts. Many had their origins as *state interoperability executive committees* (SIEC) or an equivalent required by the FCC of states that chose to manage the 700 MHz radio spectrum dedicated to interagency communications. Following September 11 and the greater focus on communications interoperability it brought, these committees have grown in many cases to represent public safety agencies statewide.

SIECs are state or statewide interoperability executive committees.

To keep regional efforts aligned with what is going on elsewhere, you may want to connect with your statewide interoperability committee. Bear in mind it may not be easy to recognize your state's interoperability committee as a separate entity from other state governance bodies. The National Summary of Statewide Communication Interoperability Plans (SCIP) published in 2009 affirmed that a one-size-fits-all approach to statewide communications governance does not exist. The report identified four common approaches states have taken to establishing interoperability governance.[64] This means you may find interoperability governance combined with or contained within other existing structures. If you want to connect with your statewide interoperability committee, one way to do so is via your Statewide Interoperability Coordinator (SWIC).[65] If you are involved in regional efforts near state borders, you should also consider participating with adjoining states' SIECs, as well.

64. See www.safecomprogram.gov/SiteCollectionDocuments/NationalSummaryofSCIPs_February2009.pdf.

65. For assistance identifying the SWIC for your State, contact your OEC Regional Coordinator. Contact information for regional coordinators is available at www.dhs.gov/files/programs/gc_1286984995227.shtm.

Statewide Interoperability Committee Resources

Federal Communications Commission (FCC):

http://wireless.fcc.gov/publicsafety/700MHz/interop.html

National Public Safety Telecommunications Council (NPSTC):

www.npstc.org/siec.jsp

Association of Public-Safety Communications Officials International, Inc. (APCO):

www.apcointl.org/frequency/interoperability.php

☐ Formalize Agreements

MOUs are suitable for small initiatives.

If your project didn't lead you to formal agreement among agencies, ongoing operations will surely take you there. Formalized agreements are necessary to establish authorities, responsibilities, and mutual expectations. In order of increasing formality, these are familiar to most public safety officials as memoranda of understanding (MOU), memoranda of agreement (MOA), inter-local agreements (ILA), intergovernmental agreements (IGA), or joint powers agreements or authorities (JPA).

Study your local and state regulations covering interagency agreements.

Each jurisdiction will have a different protocol acceptable for creating and adopting these types of agreements. Those involved in your initiative may each have different requirements, though the greater informality of MOUs lend themselves to simple agreements, particularly for smaller initiatives. Study your local and state regulations covering agreements between agencies and divisions of government.

Appendix A includes example agreements for simple and more complex sharing projects. Any agreement covering all aspects of system sharing, including governance, basic use procedures, and maintenance responsibilities, will be an extensive document.

Formal Agreement Resources

To find more information on formalized agreements, review the suite of templates produced by SAFECOM:

www.safecomprogram.gov/oecguidancedocuments/webpages/ts.aspx

☐ Make Use of the Project Communications Plan

Your project communications plan is a great resource to be carried to ongoing governance and management. It addressed sharing information among the various stakeholders who now have more of a stake than ever. Agencies, governing bodies, user and support personnel groups, and the public will need information indefinitely about the system or state of communications interoperability.

Adapt the project communications plan for the new board or council.

Governance Resources

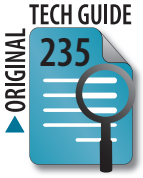
To find more information on governance structures for large, shared systems, see the supplemental resources that were produced by the National Task Force on Interoperability (NTFI): www.iafc.org/files/commComm_ntfi_supplementalLowRes.pdf; and SAFECOM www.safecomprogram.gov/library/Lists/Library/Attachments/108/GeneralGovernanceRecommendationsDHSapproved.pdf; and www.safecomprogram.gov/library/Lists/Library/Attachments/241/Establishing_Governance_to_Achieve_Statewide%20Communications%20Interoperability.pdf.

☐ Build a Sustainable Financial Structure

"Where do we get the money?"

Interoperability projects can be very expensive. Agencies regularly ask, "Where do we get the money?"

The sources are many and varied, ranging from the public agency equivalent of passing the hat (asking participants to provide for some share of costs out of their own budgets), to grants, and perhaps new forms of recurring review, such as taxes and fees. Some jurisdictions have turned to the private sector for grants and donations, although these typically fund only a small share of what are often costly projects.



Grant funding is traditionally sought for technology initiatives. The original *Law Enforcement Tech Guide* provides a whole chapter on grant management and compliance that you will find invaluable if you have received one.

In recent years there has been a significant reduction in the availability of homeland security grants. Grants are still available, but they are highly competitive and sought after for other types of projects as well. During the time when homeland security grant funding was on the rise, other existing programs diminished. Now it is just the opposite. As grant funding is on the decline, agencies are reacquainting themselves with other programs. They are evaluating the availability, distribution, legal issues, and stakeholder concerns to determine the potential value of alternative funding sources, and if it is worth assigning their limited resources to acquire them.

The total cost of system ownership can be double its purchase price.

Interoperability is a national concern and need. Federal grant programs can only fund a share of a small number of needed initiatives across the country.

☐ Plan for the Total Cost of Ownership

The total cost of ownership (TCO) for radio communications systems can be as much as twice the original system cost. A system, over its life cycle, may cost as much to operate and maintain as to purchase.

Grant Funding Resources

The SAFECOM Program maintains a web page listing potential sources of funding for communications interoperability projects:

www.safecomprogram.gov/grant/Default.aspx

Total costs of ownership for communications interoperability projects consist of:

- Development, procurement, and contracting costs
- Site development, including real estate and fixed facilities
- Hardware and software purchases, installation, configuration, and testing
- Frequency coordination and licensing
- Extended warranty and upgrade contracts
- Maintenance, support, and training costs
- Personnel costs for support staff and training overtime
- Operations costs, such as electricity and telecommunications circuits

Modern voice radio systems have an expected lifespan of about 10 years. Though user and infrastructure radios have traditionally been kept in service two or three times that long, today's sophisticated systems are increasingly computer-controlled and become obsolete much more rapidly. Manufacturers establish technology life cycles, which affect upgrade needs and, eventually, replacement.

Estimate a 10-year life cycle for modern voice radio technology.

Data communications systems are in an even greater state of flux as more and more agencies move from low-tech systems they owned, operating essentially as their voice radios did, to higher bandwidth systems, both governmental and commercially operated. A major manufacturer of equipment recommends using a 3–5 year period for calculating TCO of wireless local area networks (WLAN).[66] Consumer-grade technologies tend toward the lower end of that time range, while that built for military and public safety purposes can physically be expected to last much longer, perhaps beyond its useful life. For planning purposes, figure that the technology life cycle for data communications radio technology is closer to 5 years.

WLAN life cycles are estimated as 3–5 years.

Also, for planning purposes, estimate that ongoing operations, maintenance, and other support costs will annually cost roughly 10–20 percent of the initial cost of the technology. Costs for real estate and physical infrastructure, which can safely be estimated to have a lifespan of 30 years, may be taken from the initial costs for this estimation. However, there are ongoing costs for inspections and maintenance of infrastructure.

Ongoing costs are commonly 10–20 percent of the original technology cost.

The good news is that your agencies are probably already paying a portion of that cost in the form of maintenance and support personnel. You'll have to determine if there will be added staff and training costs in the future based on the scope of your project and the agencies' willingness to share maintenance responsibilities.

☐ Create a Long-term Funding Model

Grant funding has provided the impetus for many technology projects, but it isn't part of a long-term funding model. It's imperative that the ongoing costs of your system of systems are addressed early and in depth. Sustainable funding structures require dependable, recurring revenues that are readily available, distributable across all system costs—not just for equipment or training—and come with few, if any, legal or stakeholder challenges. Challenges that extend beyond the normal course of doing business or would take an unreasonable amount of time to address may not lend themselves well to long-term funding strategies. Ultimately, taxpayers bear the cost of providing public safety communications interoperability.

Ultimately, taxpayers bear the cost of communications interoperability.

66. "Wireless LANS – Total Cost of Ownership," Cisco Systems, Inc., 2004. See www.customcable.com/wgcc/WhitePapers/CiscoTCO.pdf.

A funding model consists of project costs, funding sources, and policies for cost sharing. Create 5- and 10-year projections of expenses and revenues. A 5-year plan is sufficient to account for budget cycles and the expiration of initial warranties. A 10-year plan has to take into account the system life cycle and the planning costs, at least, for the system's replacement.

Use 5- and 10-year projections.

Long-term funding models are as varied as the initial systems and their funding sources. The simplest are based on a handshake agreement. More complex initiatives, such as those making use of shared systems for both their intra- and interagency communications, often make use of monthly service fees to pay at least ongoing costs. Observed monthly costs range from $20 to $60 per end-user radio.

Innovation is on the upswing in funding communications interoperability projects. Fees are being assessed on consumer services, such as telephones, and vehicle registrations. General appropriations and earmarked taxes are often necessary to balance the budget. Bake sales are out.

Shared System Costs

Consider the following costs and responsibilities for shared systems.

- Infrastructure purchase – Apportioned to the jurisdiction where located.
- Mandatory system upgrades – "Must have" upgrades or system additions are paid for by the jurisdiction whose subsystem must be upgraded to coexist with the larger system; system-wide upgrades are apportioned across all jurisdictions.
- Optional system upgrades – "Nice to have" feature costs are shared between jurisdictions desiring the upgrade.
- Infrastructure maintenance costs – Apportioned across all jurisdictions.
- End-user equipment purchase – Covered individually by jurisdictions.
- End-user equipment maintenance – Covered individually by jurisdictions.

Adapted from Wake County (North Carolina) Interlocal Agreement for its 800 MHz trunked radio and CAD systems.

A big question regarding shared systems is how to determine the amount that each agency will contribute. Each cost-sharing model has its own strengths and challenges. No matter what cost-sharing model you use, chances are that one or more of the agencies involved will think they are paying too much, and that another should be contributing more. Some common models used to calculate distribution of costs among agencies for shared systems include:

Fully Distributed Maintenance Cost (FDMC): The total cost that the users incur for the annualized maintenance of the system is divided amongst the users. FDMC is a top-down approach.

Shared Infrastructure Cost (SIC): A formula is used (usually the percent of subscriber units on the system) to divide the costs of the infrastructure among all users on the system. Under this model, each agency supports its own subscriber equipment.

Shared Usage Cost (SUC): Using statistics reported by the master switch, costs are calculated and based on the percent of airtime used by each agency, calculated against the total air usage time for that period.

Per Capita Costs Basis (PCCB): Each agency pays in accordance to their per capita, as determined by the local planning council (LPC) for the area.

Public/private partnerships: The costs are shared between public and private entities, such as commercial wireless carriers, so the parties have a mutually beneficial relationship. Examples of this can include co-location of public radio infrastructure on commercial wireless towers, use of existing private facilities, private security company access to radio systems, etc. In addition, commercial wireless carriers can pay a fee to use public facility assets and these funds can then be applied to the ongoing sustainment.

> The pursuit of perfection often impedes improvement.
> —*George Will*

Periodically review the governance and financial structures, as well as policies and procedures.

Create a Review Process

As the final piece of setting up governance and management, create a process for periodic review of all aspects of the initiative—from the governance structure and its membership to the financial structure. Focus particularly on the system policies and procedures that fuel communications interoperability. Reviews bring out needed updates and validate those parts that don't need changes. They provide a means of continuous improvement without participants becoming lost in a pursuit of perfection.

Have a wish list for surprise year-end opportunities.

Annual reviews are usually sufficient. Stagger individual reviews throughout the year to make them less of a chore, sharing ongoing work across participants. For example, January is a good time for strategic reviews to capture the enthusiasm of the new year during a slower period for most agencies. The financial structure and budgets may be reviewed shortly before the end of the participants' fiscal year—presuming they are similar—to identify needs that might be met through year-end funding, and to prepare a budget for the upcoming fiscal year, if needed.

Spread reviews through the year and responsibility across the participants.

Policies and procedures should also be reviewed on a rotating schedule throughout the year to spread the work. The User and Technical Committees appropriately bear the bulk of the effort, with the Board, in whole or part, annually reviewing management policies and procedures.

CHAPTER 12

Develop Policies and Procedures

What: Formalized interagency agreements are needed on how the system will be maintained and used, integrating the National Incident Management System.

Why: Interagency communications policies and procedures establish how technology is to be used to achieve interoperability. Integration of NIMS ensures an operational focus compatible with incident management systems with other potential partners beyond the initiative.

Who: The system governance board approves acceptable policies and procedures developed by the User and Technical Committees.

When: Develop policies and procedures early in the project, continuing through cycles of continuous improvement after implementation.

In Chapter 10, we briefly touched on the creation of policies and standard operating procedures (SOP). We noted that they evolve from SOPs already existing within or, potentially, already between partnering agencies that influenced your project needs statements. During implementation, some are ideally further defined and executed through initial system training. The bulk of your policies and procedures, however, are likely to grow as the system is used more and more.

We refer here to policies as proscriptive rules and procedures as practical guidance for how something is done. Policies may make procedures mandatory, but SOPs aren't necessarily so.

Integrate NIMS into SOPs

SAFECOM's *Interoperability Continuum* addresses SOPs as one of its five key dimensions in achieving interoperability. Standard operating procedures based on the National Incident Management System (NIMS)[67] are identified as an indicator of advanced communications interoperability.

Central to NIMS integration into policies and procedures is the Incident Command System (ICS). Policies and procedures based on ICS, incorporating its structure, conventions, and operational principles, bring commonality to the way different agencies work.

NIMS-integrated SOPs lead to interoperability.

Create policies and procedures for routine and targeted capabilities using a standard model adopted by the governing body. Address technical and operational aspects of the system, integrating NIMS throughout. This approach assures the greatest communications interoperability, plus compatibility with neighbors far and wide.

We will cover communications aspects of NIMS ICS in detail shortly.

National Priorities:
–NIMS
–Information sharing
–Communications interoperability

Focus on Routine and Targeted Capabilities

Policies and procedures for communications systems, first and foremost, provide for agencies' day-to-day operational needs. Procedures that are used regularly become part of a responder's natural reactions. All emergency response disciplines recognize that, under the stress, people perform as trained—for better and worse. The classic, if tragic, story in law enforcement is of the officer found shot with empty cartridge cases in his pocket, having spent hours on the shooting range practicing "procedures" that had nothing to do with—and were counterproductive to—surviving a shootout.

People perform as trained—for better and worse.

During the stress of emergencies, responders will most reliably perform the tactics they have learned, exercised, and used daily. Interagency communications procedures are only effective if used. They are most likely to be used if they are part of daily or, at least, very regular practice.

67. See Chapter 3, **Operability—Job #1**.

Lay the groundwork for automatic behaviors during emergencies by establishing routine interagency procedures. Make the less common ones memorable by making them simple, by creating "cheat sheets" for easy reference, and by practicing them during exercises. Don't presume that every proscriptive policy and each procedure established will immediately become part of every responder's repertoire.

Tactics and tools used daily will be most reliable during unusual emergencies.

Targeted Capabilities

Homeland Security Presidential Directive 8 (HSPD-8), "National Preparedness," was released in late 2003, and then updated in March 2011. The update also served to rescind HSPD-8 Annex I (National Planning).[68] The initial purpose of HSPD-8—to strengthen preparedness capabilities of all levels of government to terrorist attacks, major disasters, and other emergencies—remains unchanged.

The original HSPD-8 initiated the development of a national preparedness goal that included readiness metrics and full implementation of a closely coordinated interagency grant process for first responder preparedness assistance. The interim National Preparedness Goal was issued in 2005 and then replaced by the National Preparedness Guidelines (Guidelines) in September 2007.[69] The Guidelines reflect policy direction outlined in the 2010 National Security Strategy and "define what it means for the Nation to be prepared for all hazards."[70] Four of the eight national priorities articulated in the *Guidelines* are particularly relevant here: implementation of NIMS, strengthening of information sharing and collaboration capabilities, strengthening communications interoperability, and implementing the National Infrastructure Protection Plan (NIPP). The Guidelines use an approach called *Capabilities-based Planning* to reach the National Preparedness Vision, with 15 standardized *National Planning Scenarios* (NPS), a *Universal Task List* (UTL) to reference tasks performed by all levels of government and different disciplines during incidents, and a *Target Capabilities List* (TCL) identifying capabilities needed to perform the tasks.

68. See www.whitehouse.gov/news/releases/2003/12/20031217-6.html.
69. See www.dhs.gov/xabout/laws/gc_1215444247124.shtm.
70. See www.dhs.gov/xlibrary/assets/National_Preparedness_Guidelines.pdf.

Operational plans are to be built upon SOPs consistent with NIMS.

In March 2008, the *National Response Framework* (NRF) replaced the National Response Plan originally issued in 2004. The NRF provides a framework for all levels of government to align their strategic and operational plans. The effectiveness of the Incident Annexes carried over from the National Response Plan is expected to benefit from the improved coordination.[71] Operational plans are supported by or built upon SOPs and are intended to be consistent with NIMS guidelines, standards, and protocols.[72] Emergency planners are expected to identify tasks from the UTL that their organizations need to perform based on their assigned roles and mission. The TCL descriptions are used to determine the capabilities needed to accomplish these tasks, variously and by different response elements. Operational and strategic plans are specific to the National Planning Scenarios.

Interoperable communications is one of five capabilities common to all mission areas.

Currently, there are 37 capabilities in the list, 32 of which are grouped into four mission areas: **prevent**, **protect**, **respond**, and **recover**. The remaining five are capabilities common to all mission areas. Communications is second among the five common capabilities.

Since first introduced in 2005, work has been accomplished to define conditions and standards for each universal task, as well as performance measures and metrics to assess capabilities. As capability assessments occur, gradual but continuous improvement should result. Measuring communications interoperability is addressed in Chapter 15.

Throughout this book, we address communications interoperability capabilities generally. They are not listed here for security purposes. Adoption and incorporation of NIMS and capabilities listed in the TCL will lead to advanced interagency communications supporting common response processes.

Specific information on the National Response Framework tasks and capabilities can be found in the NRF Resource Center and the U.S. Department of Homeland Security's Lessons Learned Information Sharing website.[73]

71. To support users of the Framework, the Department of Homeland Security has created an online NRF Resource Center, available at www.fema.gov/NRF. See also www.fema.gov/incident-annexes.

72. The National Response Plan and National Incident Management System were established by Homeland Security Presidential Directive 5: Management of Domestic Incidents (HSPD-5). See www.dhs.gov/xabout/laws/gc_1214592333605.shtm.

73. The Lessons Learned Information Sharing website is only available to emergency response providers and homeland security officials. Registration is required and eligibility is verified. See www.llis.dhs.gov.

Establish and Use a Standard Method

Policies and procedures governing interagency communications are crucial for interoperability. Agencies that have adopted a standard method for their creation have found them easier to develop and maintain. Two examples come from the northern latitudes: Minneapolis-St. Paul, Minnesota, and the State of Montana.

A standard method for procedures simplifies their creation and maintenance.

Shared Systems in the Twin Cities

The Minnesota Statewide Radio Board oversees a statewide radio system shared among many agencies. The Allied Radio Matrix for Emergency Response (ARMER) is the nucleus of a growing statewide system.[74] The Board has used a standardized template and approach to create an extensive set of standards, protocols, and procedures.

The comprehensive standards document, which is available online,[75] includes a template showing and describing seven elements:

- A document title, control, and approvals block
- A *purpose* or *objective* statement
- A *technical background* statement describing capabilities and constraints under which the standard, protocol, or procedure is used
- An *operational context* statement addressing when it is appropriate
- A *recommended protocol/standard* statement addressing related criteria that qualify use of the one being established
- The *recommended procedure*, itself, describing how the task is performed, including individual steps and locations of reference documents
- A *management* statement describing who is responsible for supervising or managing this procedure

Appendix B contains an example from the Statewide Radio Board document that addresses patching of shared channels in the region to the system.

74. *Standard Operation Procedures Case Study: Minnesota*, DHS, September 2011.

75. Governance of ARMER was transferred from the Metropolitan Emergency Services Board. Information on ARMER is available through the Statewide Radio Board at www.armer.state.mn.us.

Shared Channels under the Big Sky

The Montana shared channels plan includes policies, procedures, and practical use examples.

The State of Montana has a comprehensive, shared channels plan widely used by local, state, and federal responders in the state.[76] It defines 14 channels available for use across disciplines, incorporates ICS throughout, and provides practical examples of use. The bulk of the plan addresses practical applications, with the formal plans, plus policies and procedures, included as appendixes.

The formal plans for each channel are simple, one-page documents describing the purpose of the channel, eligibility for use, and basic usage standards. More detailed policies and procedures documents are provided for each separately, addressing in a standardized form oversight, eligibility, licensing and authorization, operations, requirements, procedures, and channel use discipline.

The Montana shared channels plan demonstrates a standardized method for creating policies and procedures, coupled with practical demonstrations of use.

Create Technical Policies and Procedures

Following a standardized method, you can create policies and procedures that both serve your system of systems and are manageable. Both technical and operational SOPs will be needed. The Technical and User Committees of the governing body are commonly tasked with responsibility to create the SOPs, carry them through approval and adoption, and maintain them over time.

Many technical SOPs can be developed over time, shaped by your system and needs. Some of the more common ones include:

- Equipment Management and Deployment[77]
- Standard Equipment Configurations
- Maintenance of Radio Caches
- Gateway Configuration, Maintenance, Deployment, and Use

76. *Montana Mutual Aid and Common Frequencies*, State of Montana, 2011. The 2005 version was a minor update to the 1994 edition written by the original author of this tech guide. See http://pssb.mt.gov/mutual_aid_manual.mcpx.

77. Communications Asset Survey and Mapping (CASM) is a tool used by states as well as many local jurisdictions to support public safety communications needs for inventory management, as an adjunct to TICP and NIMS-ICS (Form 217). For more information contact DHS Office of Emergency Communications at oec@hq.dhs.gov.

- Outage Responsibilities and Standards for Repairs
- Availability of Spare Equipment
- Preventive Maintenance
- Notification of Maintenance Activities

Technical maintenance needs are addressed in Chapter 14, **Maintain the Technology**, which discusses some specific activities where technical SOPs may be necessary.

Create Operational Policies and Procedures

Operational policies and procedures address how the technology is put to work. Many will arise from existing SOPs, but you will need to develop others that extend the interagency communications capabilities through your new system.

The highest levels of interoperability are achieved through integration of the NIMS into procedures used regionally across participating jurisdictions.

SAFECOM Template Models

Let's take a closer look at what the SAFECOM template suite has to offer in the area of SOP development.

But before we do, we should note that SAFECOM modeled this series of SOP templates after none other than the subjects in our Minnesota case study. The Metropolitan Emergency Services Board (MESB) that originally governed the ARMER system set a strong foundation for SOP development, which passed through to the Statewide Radio Board. The SOPs developed were so effective that the Minnesota Department of Public Safety Performance Review of the I-35W Bridge Collapse in 2007 found "no major adjustments were needed to the SOPs during the response." In fact, the alignment and early development of the SOPs are credited for the region's ability to maintain order throughout the incident.

The SAFECOM templates for SOP development consist of a series SOPs that govern some common radio system resources used to achieve interoperability. These include:

- Shared Channels
- Shared Systems
- Mobile Gateways
- Console Patch
- Radio Cache

The templates consist of two parts. The first part provides easy-to-understand instructions and examples that will help agencies fill in the second part—a customizable SOP template that can be tailored to meet the user's needs. These templates are great tools but the effectiveness of SOPs will only be as high as the level of collaboration used to write them. Make sure the right people are at the table when writing your SOPs.[78]

ICS Communications Unit

Under ICS, the Communications Unit is under the Logistics Section.

Under NIMS ICS, the Communications Unit is established as a logistical service function. It is responsible for establishing the Incident Communications Center (ICC), which is typically part of the Incident Command Post, and creating the Incident Communications Plan.[79] The communications unit leader (COML) is the key person to plan and manage the technical and operational aspects of the communications function during an incident or event. The COML is responsible for participating in incident planning meetings to:

- Determine the feasibility of providing the required communications support
- Provide operational and technical information on communications equipment available for the incident
- Provide operational and technical information on communications equipment capabilities and restrictions[80]

78. www.safecomprogram.gov/oecguidancedocuments/webpages/ts.aspx.

79. ICS uses standardized forms. The Incident Communications Plan, described further in this chapter, is based on form ICS 205. See www.fema.gov/pdf/emergency/nims/ics_forms_2010.pdf.

80. Adapted from current editions of National Wildfire Coordinating Group task books. FEMA position task books are available at http://training.fema.gov/position%20specific%20taskbooks/taskbook_list.asp.

The Communications Unit is composed of four different positions, as needed: The COML, communications technicians (COMT), radio operators (RADO), and incident communications center manager (INCM). These positions are only filled when needed. Appendix C provides task lists from NIMS-compliant source material for each of these positions.

The Communications Unit includes a leader, technicians, radio operators, and ICC managers.

Integrated communications is an original, fundamental tenet of ICS. Policies and procedures for use of the ICS Communications Unit during larger emergencies are important for communications interoperability. Objective 5 of the National Emergency Communications Plan (NECP) targets communications unit positions and highlights gaps in training, technical expertise, and response capabilities.[81] Integrating communications unit positions, specifically the COML and COMT, in NECP goal validation events has generated positive responses from the evaluators. An example that has proven effective is including the COML in planning briefings.

Incident Dispatch Teams

In the public safety field, incident dispatch teams have grown in popularity over the past few years. In law enforcement, they are more commonly known as tactical dispatch teams for their role in supporting SWAT team operations.

By either name, incident dispatchers and their supervisors would staff the ICS RADO and INCM positions, respectively, in a NIMS-based response. During large emergencies, an on-scene communications center is crucial.

Consider establishing policies and procedures for incident dispatch teams as part of your Communications Unit.

81. Standardized training is available nationwide for a variety of communications unit positions including COML and COMT; see http://training.fema.gov and www.dhs.gov/files/programs/gc_1286984043354.shtm.

Incident Dispatch Resources

At least two organizations exist for the benefit of incident dispatch.

The California Tactical Dispatcher Association is focused primarily on police operations: www.tacticaldispatch.com/

Incidentdispatch.net, also based in California, is more broadly focused on all-risk incident communications: www.incidentdispatch.net/

Emergency Traffic

Almost all aspects of communications continue to be problematic, from initial notification to tactical operations.

—Arlington County, VA 9/11 After-Action Report

From a very practical standpoint, communications procedures continue to be problematic. Improved interagency communications depends on developing some of the most basic emergency procedures. For example, consider how traffic is held or cleared on a channel for other, higher priority emergency traffic.

Most agencies have procedures for declaring "emergency traffic only" on a channel. In routine operations, dispatchers are charged with the responsibility on dispatch channels of declaring it or accepting an announcement from another user. They are in charge of controlling the network, in effect, and opening it back up for regular traffic.

Procedures are also needed for emergency traffic on channels that dispatchers don't manage. Tactical channels used on-scene are in equally high need of procedural definition of who declares "emergency traffic," who controls the channel, and how it's cleared. Typically, the highest-ranking ICS position on the channel bears the responsibility.

Channel Span of Control

Very similar to the ICS principle of maintaining a manageable span of control in supervision, channel span of control procedures are important. The history of emergency response is replete with stories of responders in dire circumstances who couldn't get access to a channel because of too much traffic. One of the most tragic occurred in Hackensack, New Jersey.

In the 135-year history of the Hackensack Fire Department, nine firefighters have made the ultimate sacrifice. Four have died in motor vehicle accidents. Five perished during one fire on July 1, 1988. Two firefighters—who initially survived the collapse of a bowstring truss ceiling that claimed the lives of the others—were trapped inside where they were unable to communicate their situation due, in part, to the channel being overloaded with other tactical, command, and dispatch traffic.

Maintenance of a manageable span of control on a radio channel enforces the more general ICS management principle. Use of tactical channels removes some share of other incident traffic from broader dispatch and response channels. Ideally, only a single supervisor and subordinates would operate on a single channel. Any more than that and responders have to decipher traffic not intended for them, risk mixed orders, and compete for the channel when they have emergency traffic. The volume of traffic on overloaded channels has caused more than one responder to turn the volume down or radio off in order to have a moment to think or converse with others.

Operations with extremely compressed timeframes, such as SWAT incidents, advanced life support, and most firefighting require simple, direct, and immediate communications capabilities. This can only be provided by maintaining a manageable channel span of control.

Create policies and procedures that move incident traffic from cluttered channels to operational and tactical channels organized in a manner similar to the incident organizational structure.

> Communications often becomes the 'fall guy' for organizational problems. An excessive number of responders attempting to talk to the IC* (generally all at once), compressed time, getting behind and chasing the incident problem, playing 'catch up,' and general operational confusion can quickly beat up and overwhelm any incident commo [communications] plan/system. . . . Any part of the system operating beyond their effective span of control (five to six) will almost instantly develop commo problems. The way to fix the commo problem is to fix the span-of-control problem, and (bingo!) the commo settles down and becomes normal.
>
> — *Fire Command*
> *Chief Alan Brunacini,*
> *Phoenix (AZ) Fire Department*
> **Incident Commander*

Standard Language

Much of what passes as poor communications is actually *mis*communications. NIMS ICS and its predecessors identify as its first management characteristic the use of common terminology for organizational elements, position titles, resources, and facilities. One of the most important policies that can be established for interagency communications is common terminology to be used by responders, further reinforced through procedures.

Common terminology, resources definitions, and plain language are crucial for communications interoperability.

In addition, standard resource definitions improve interoperability. From a communications standpoint, naming conventions for channels and other communications resources are critical to get standardized across jurisdictions. It's unfortunately common for agencies to be working together with a common radio channel at their disposal that they're unaware of or that they have each named so differently that nobody would associate them. Some regions go so far as to establish not only standard names for shared channels or talk groups, but also standard programmed positions in the radios for interagency resources.

Lastly, the most important policy that can be adopted to improve interagency communications is the use of plain language during major disasters and exercises. Typically, these types of events are multiagency, multijurisdictional, and multidisciplinary. To achieve interoperability in these circumstances, it is essential to eliminate the use of codes and jargon. This is a simple idea, but every vocation and avocation has its own terminology. When these diverge across agencies and disciplines, responders don't communicate and response is hindered. [82]

There has been ongoing controversy over requiring use of plain language for internal operations. The NIMS integration center does not require plain language during internal operations; however, it highly encourages it[83] because people tend to perform the same way in an emergency situation that they do on a daily basis.

Communications-Order Model

Another communications best practice that has proven effective is a *communications-order model* that provides positive message acknowledgement. This is a basic process that can work with any medium, voice or data, but is most clearly seen with first responder push-to-talk radio communications. It's simple and we do it in our daily lives when we're communicating best.

82. Current plain language guidance can be found in the NIMS Resource Center at www.fema.gov/emergency/nims/.

83. The importance of using plain language was further documented in the National Emergency Communications Plan (www.safecomprogram.gov/SAFECOM/natlemergencycommplan/) and noted as an FY2008 Compliance Objective of the National Incident Management System (NIMS).

Five steps are involved.

1. Calling unit gives the name of the called unit, followed by its own.
2. The called unit responds with the reverse.
3. The calling unit transmits its message.
4. The called unit briefly restates the message to show understanding.
5. If the message was received correctly, the calling unit responds with an affirmative acknowledgment, otherwise responds "Negative" and repeats the message.

Some jurisdictions reverse the order of whose "name" goes first. A standard convention is most important, though there's bound to be those border issues where one convention butts into the other, confusing everyone who doesn't recognize the callers' voices and is trying to figure out what's going on. While there is no definitive standard, we suggest the sequence above. It's used by many public safety agencies, the U.S. Army, and air traffic controllers, which is good enough for us!

Positive message acknowledgment is good communications.

The keys to the communications-order model are convention and positive message acknowledgment. The sender knows the message was received as intended. With practice, it can be done efficiently, with a fraction of the airtime necessary for repeated and missed messages.

Operational Unit Reporting

The final example of a communications SOP for operational purposes is standardized unit reporting. Beyond the obvious value of clearly communicating who's talking and what the message is, status information can be transmitted efficiently that provides greater context for all parties involved in the conversation, active or not. Standardized reporting during multiagency response when confusion often reigns can be established through policies and procedures.

Development of unit reporting procedures gets operations folks talking about operational needs and uses of the system.

A simple example is the transmission of location and status by reporting units—typically those in the field—once during a sequence of transmissions. While modern trunked radio and automatic vehicle location (AVL) systems capture some of this information, nothing is so simple and effective for all participants as a simple voice transmission. Not everyone who "needs to know" will be near a CAD display or using AVL-enabled radios (essentially only mobiles). A simple "Available at staging" statement says a lot.

Operational unit reporting procedures across agencies are powerful tools to flesh out the system of systems by getting field operations staff talking about what they need to talk about.

Build Incident Communications Plan Templates

SOPs drive the development of the incident communications plans. Under ICS, the Incident Communications Plan is documented using the ICS 205 form, which is itself part of the formal Incident Action Plan (IAP). The IAP is a collection of forms, starting with the ICS 201 (Incident Briefing), plus supporting material.

ICS 205

Templates are useful, and can be customized for large events.

The Incident Communications Plan—sometimes called the Incident *Radio* Communications Plan—is specific to an incident due to its unique geographic location and extent, the type of operations supported, and the scale of response. Templates are useful tools in preparing for response.[84]

Plans do have to be customized by a Communications Unit during larger emergencies, however. What constitutes a large emergency is jurisdiction-dependent. Basically, any response requiring more than a couple dozen responders needs an on-scene, incident communications center of some form—and a communications plan tweaked somewhat to fit the incident.

The ICS 205 identifies communications resources, their functional assignments (e.g., "Talkgroup X is assigned to Division A command"), and technical parameters of the resource, such as frequencies and tones for conventional channels. From an operational standpoint, the ICS 205 says a lot about the participating agencies and the incident command structure. A well-done Incident Communications Plan both reflects and reinforces the command structure. Supplemental material may describe such things as usage priorities, procedures, and protocols.

The diagram in Figure 12-1 on page 232 depicts a realistic organizational chart identifying responders to a hypothetical event by their function. This is highly preferred to identification by agency, which tells the user nothing about what they're doing.

84. FEMA has standardized numerous ICS forms adapted from the National Wildfire Coordinating Group, a long-organized group of governmental agencies with wildland firefighting responsibilities. See www.fema.gov/pdf/emergency/nims/ics_forms_2010.pdf.

In this example, each line between functional elements represents a communications path of some sort. During emergencies, these are typically radio channels—whether discrete frequencies in a conventional system, talkgroups in a trunked system, or even composite channels as may occur when multiple frequencies and talk groups are patched together with a gateway.

Consider an example. The "Law Enforcement Branch" director and each of the team leaders and group supervisors are connected by a common line, or channel, of some form. The communications plan has to identify how that connection is made. Typically, some radio channel would be assigned for "Law Enforcement Branch Command," which is represented by that line. The ICS 205 for this scenario would, figuratively, describe how each of those interconnecting lines is supported with communications.

Communications plans have Branch directors, group supervisors, and team leaders as standard ICS position titles.

The experienced responder will notice that the chart in Figure 12-1 on page 232 stops at a certain level of detail and doesn't depict the tactical channels that would be used within many of the indicated operational elements. The diagram is simplified for the sake of discussion, whereas an actual incident response with those operational elements would likely involve more than a hundred responders. The ICS 205 for the scenario—whether as a template or an actual incident plan—would identify all communications resources to be used to support the response.

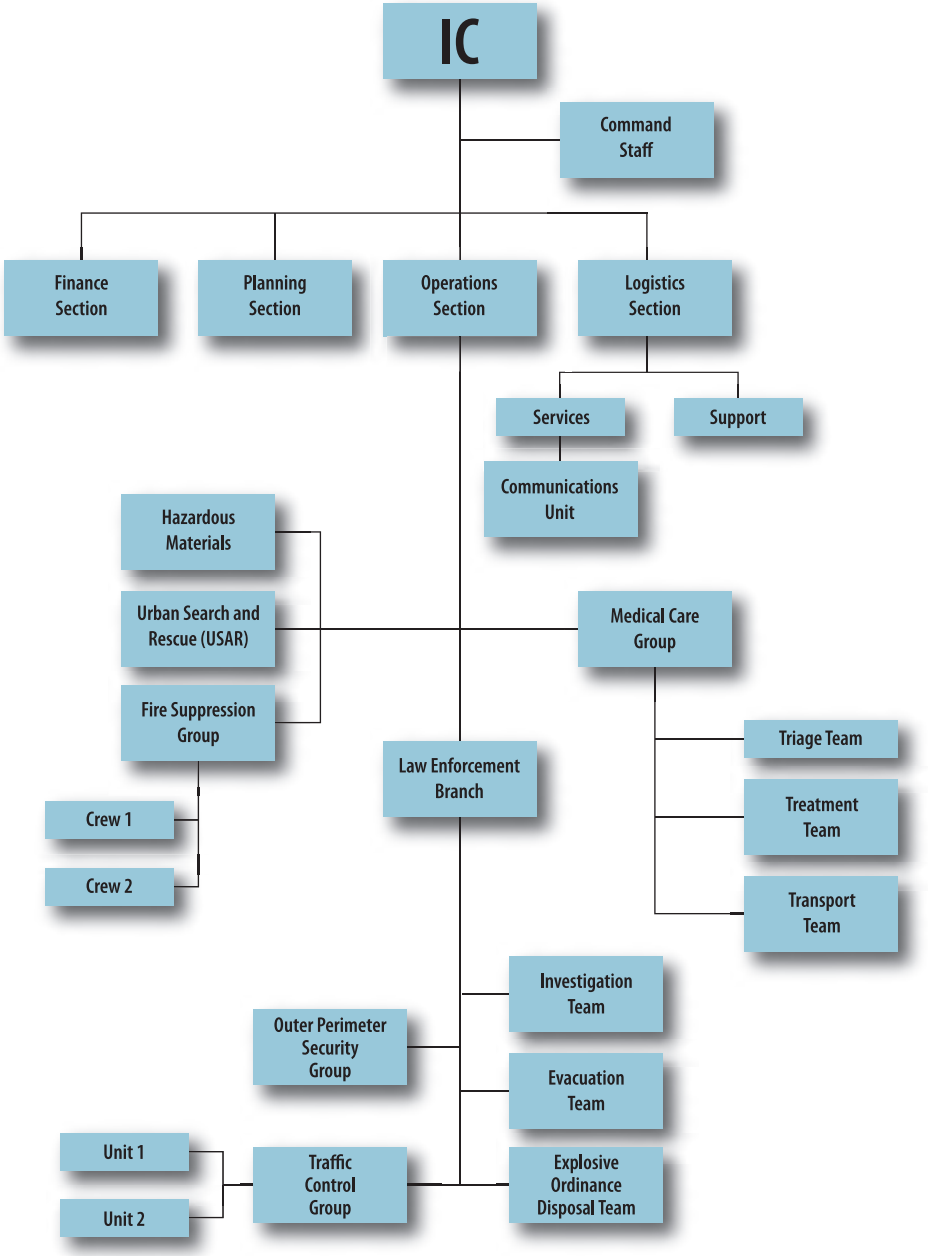
Tactical Interoperable Communications Plans

Under the Federal Fiscal Year 2005 Homeland Security Grant Program,[85] all designated Urban Area Security Initiative (UASI) regions and one metropolitan area in each state without a UASI region, were required to complete a *tactical interoperable communications plan*. This plan was intended to identify how the region would support operational response within an hour of an incident occurring. The elements of the required plans may be instructional to all agencies, whether or not they were required to complete them as a condition of homeland security funding.

Tactical interoperable communications plans are a requirement of some homeland security grant funding.

85. See www.fema.gov/government/grant/hsgp/index.shtm.

Figure 12-1: Sample Improvised Explosive Device (IED) Scenario Organizational Chart



Federal guidance for these plans suggested including the following elements:

- Background, describing the urban area and how tactical interoperable communications would be governed in the region
- An equipment and capabilities inventory, including points of contact for activating and supporting resources
- Tactical interoperable communications policies and procedures
- Incident communications plans matching resource to response structures
- NIMS-compliant training planned for Communications Unit Leaders
- Appendixes that further document details

These topical areas outline well the information needed for incident communications planning.

"Well-documented and consistent Standard Operating Procedures give our public safety responders the best opportunity to go home safe and sound at the end of their shift."

– *Tom Johnson, Minnesota Statewide Interoperability Coordinator*

CHAPTER 13

Train and Exercise

What: Train and exercise refers to the process of instilling skills and improving performance for achieving communications interoperability.

Why: As part of the system of systems for interoperability, users have to be prepared for routine and targeted capabilities in the context that skills will actually be used.

Who: The User and Technical Committees are responsible for guiding development of training and exercises for interagency systems.

When: Start training and doing realistic exercises during implementation, in a process of continuous improvement through the system's life cycle.

All the policies and procedures created to improve interagency communications are useless unless they are put to work. Training and its practical counterpart, exercises, are required for any system of systems to work during routine events, special task force operations, or large-scale emergencies.

> Not every difficult and dangerous thing is suitable for training, but only that which is conducive to success in achieving the object of our effort.
> —*Epictetus*

Focus on both Routine and Targeted Capabilities

As noted previously, the most well-executed tactics are those used and practiced on a daily basis. Communications interoperability is achieved, foremost, through the regular use of interagency capabilities on a routine basis.

Instill the best practices for response during emergencies large and small by building them into basic training and in-service programs, as well as into exercises that give responders even greater ability to use the communications capabilities during realistic circumstances. Meld the target capabilities of the *National Preparedness Guidelines* (previously contained in the National Response Plan)[86] into training for both routine and extraordinary events, to assure agencies involved in your initiative can leverage what they do daily for even larger emergencies. Recognizing that many capabilities will grow over time, use a process of continual improvement to chart progress.

> A good plan today is better than a perfect plan tomorrow.
> — *General George S. Patton*

86. The National Response Framework (NRF) replaced the National Response Plan (NRP) in March 2008. This Framework commits the federal government, in partnership with local, tribal, and state governments and the private sector, to complete both strategic and operational plans for the incident scenarios specified in the National Preparedness Guidelines. The NRF is available at www.fema.gov/pdf/emergency/nrf/nrf-core.pdf.

Train in Context

The most effective method of training adults in practical skills is by doing it within the context of how the skills will actually be used. For example, the training mentioned previously that led police officers to pocket empty cartridge cases has given way to realistic, tactical training in which officers are required to seek cover, distinguish threatening from nonthreatening targets, and shoot effectively under added distractions. This training in the context of how skills will be used is very effective and applicable in communications training.

I hear and I forget. I see and I remember. I do and I understand.
—*Confucius*

In effect, end users aren't trained to use radios—they're trained to communicate while doing their jobs. That may seem like a subtle distinction, but in practice it means that communications training is most effective when it is embedded within other training—not conducted in isolation.

Building on the above example, realistic police communications training would require an officer to request assistance by radio while engaging targets on the range. Or a firefighter reporting completion after ventilating a roof with a power saw.

Exercises provide the means to stress-test the entire system of systems.

Use Standardized Exercise and Evaluation Processes

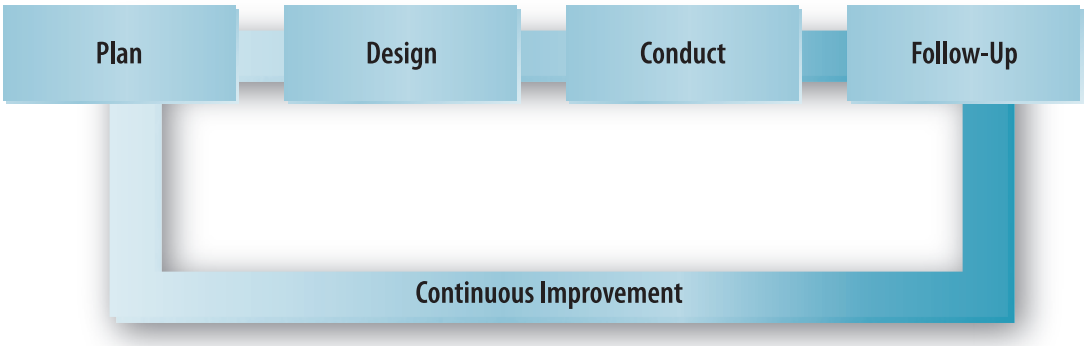
Exercises offer the opportunity to train skills in context. The use of a standardized exercise process, coupled with meaningful evaluations, provide the means to train and progressively develop skills.

From the perspective of communications interoperability, exercises provide an ideal opportunity to stress test the entire system, including the hardware, the software, and the "liveware." A standardized exercise program includes a progressive set of exercises that are each appropriately evaluated, with results incorporated back into the program for further training.

The U.S. Department of Homeland Security's Homeland Security Exercise and Evaluation Program[87] (HSEEP) provides extensive guidance for designing, conducting, and evaluating exercises. Discussion- and operations-based exercises are addressed in detail. The program underwent revisions in 2007 to further incorporate the National Planning Scenarios, Universal Task List, and Target Capabilities List of what was, at the time, the National Response Plan. Not only does the program provide useful guidance, its use helps jurisdictions meet requirements for grant funding.

87. See the HSEEP at https://hseep.dhs.gov/pages/1001_HSEEP7.aspx.

Figure 13-1: Tabletop Exercise Methodology Development Process



Discussion-based Exercises

HSEEP addresses four types of discussion-based exercises: **seminars**, **workshops**, **tabletop exercises**, and **games**. Seminars and workshops are familiar to most people, while tabletop exercises and games are less so. According to HSEEP, operational simulation games are an increasingly sophisticated and useful component of exercise programs. They seem to currently offer little in the way of communications training suitable for first responders, however.

Tabletop exercises provide the means to master script for operations-based exercises.

Tabletop exercises are probably more familiar in emergency training than are games or other automated simulations. Tabletops offer an opportunity to first introduce new policies and procedures, identify disconnects as they are tested through discussion, and then master scripts that might be further tested operationally.

With all the SAFECOM tools and templates we have introduced in this guide so far, we are not finished yet. SAFECOM also developed the Communications-Specific Tabletop Exercise Methodology to help plan, design, and conduct tabletop exercises that target communications.[88] It uses a step-by-step approach to help agencies develop effective exercises that are in alignment with HSEEP guidelines and other communications best practices (see Figure 13-1). Similar to the other SAFECOM tools, the methodology encourages collaboration among users and customization of exercises.

88. See www.safecomprogram.gov/SiteCollectionDocuments/CommunicationsSpecificTabletopExerciseMethodology.pdf.

Using the guide will help create tabletop exercises that:

- are realistic exercise scenarios;
- are realistic tests of actual response processes and procedures;
- generate usable exercise results;
- enable the identification and implementation of effective interoperable communications solutions;
- identify interoperability capabilities and gaps in existing processes.

Agencies that commit to using the Communications-Specific Tabletop Exercise Methodology to conduct exercises on an annual or semiannual basis will establish a process geared toward continuous improvement.

Operations-based Exercises

Operations-based exercises provide training in context.

As the name and distinction implies, operations-based exercises take participants to the field for actual training and practice. They provide the means to validate policies and procedures, while testing the technology as well. Three types of operations-based exercises are identified by HSEEP: **drills**, **functional exercises**, and **full-scale exercises.**

Drills are limited exercises.

Drills are limited in scope, testing one part of the system in isolation, although as realistically as possible. An example for communications may be a drill of a technician team responsible for the deployment of field gateways. Procedures that could only have been discussed during a tabletop exercise can be tested in more realistic circumstances, although still in isolation from a larger response system. This allows system managers and planners an opportunity to evaluate the procedures—as well as the drill design—for subsequent improvements.

A *functional exercise* along the same lines might bring a special operations team and the technicians to the field with a mobile command post to test not only deployment and setup, but also further use. The exercise is still limited in scope and evaluation is key to the process of continuous improvement. HSEEP notes that functional exercises are generally designed to exercise the direction and control of resources, rather than systems. In our example, the gateway would not be thoroughly tested for functionality, capacity, and coverage, but rather for its appropriate deployment and operational command.

Full-scale exercises are, by definition, multijurisdictional exercises that bring out a full response system. Communications is tested as a part of a larger effort. This provides realism that exercises the communications interoperability system of systems, as a whole, in the context of how it's used during near-real operations. Full-scale exercises are intended to stress-test systems under realistic circumstances and timeframes.

Full-scale exercises stress-test entire systems.

Evaluations

As noted, exercise evaluations are crucial. They are appropriately designed, planned, and carried out with as much attention to detail as the rest of the exercise. HSEEP provides an entire volume addressing the process.[89] Key elements include the use of a debriefing for planners, facilitators, controllers, and evaluators and a "hot wash" for all others. The hot wash follows the exercise immediately, while multiple debriefings may be necessary to capture observations and document details from multiple sites. Debriefs and hot washes are used in evaluation of both discussion- and operations-based exercises.

Exercise evaluations are necessary for a process of continuous improvement.

An *After-action Analysis and Report* (AAR) captures details more broadly for the record and recommends improvements. Under HSEEP, they are prepared for all exercises except workshops and seminars, where a summary report suffices.

Communications is not an independent element of emergency response that can be adequately exercised and evaluated in isolation. It is only through integrated exercises that it can be trained in context, tested, evaluated, and set for continuous improvements. Interagency communications can likewise only be exercised adequately and evaluated critically through multiagency efforts.

89. *Homeland Security Exercise and Evaluation Program, Volume III: Exercise Evaluation and Improvement*, U.S. Department of Homeland Security. Available at https://hseep.dhs.gov/pages/1001_HSEEP7.aspx.

CHAPTER 14

Maintain the Technology

What: The goal of the ongoing work is to keep technical components of the system operational over its life cycle.

Why: Without maintenance, technology deteriorates over time. Optimal performance of technology is achieved through regular and preventive maintenance, coupled with a proactive process of managing changes to it.

Who: Ultimately, the system's governing body is responsible for identifying which agency, agencies, or vendors will maintain different technical components of the system.

When: Start your system's maintenance from the day the technology is installed, throughout the system's life cycle.

Maintaining your communications interoperability system of systems involves not only the human components, but also the technology they use. Upon implementation, your system technicians immediately went into maintenance mode. While new technology, once up and running smoothly, requires less initial maintenance, there are aspects that have to be maintained *continuously*.

Identify Responsibilities

Start the maintenance process by identifying responsibilities for each technological component of the system and each job that has to be done. Your implementation plan provides a good starting point for this effort. Address the roles and responsibilities of each participating agency's technical staff, equipment installers (if independent), local radio shops that are to be used, and other network maintainers. This last category includes maintenance functions of leased telecommunications circuits, if you have used them.

Use a matrix to chart responsibilities.

Use a matrix of responsibilities that is charted by agency or organization. Cooperative systems being built around the country often have a particularly complex set of roles and responsibilities. Make them clear to reduce confusion and potential conflicts, while maintaining the highest level of system performance.

Create a Technical Continuity of Operations Plan

Near the top of the list of things to do in maintaining the technology is to create a continuity of operations plan. Technical staff are in the best position to manage risks naturally faced with the technology.

A technical continuity of operations plan addresses the following:

- Risks, including their likelihood, severity, areas of impact, and mitigation
- Points of contact for managing outages
- Procedures for notifying user agencies of outages
- Technical adaptations to maintain system performance

During large-scale emergencies and disasters, information about impacts on communications systems is vital. Prepare the continuity of operations plan to inform incident management staff of immediate or imminent effects on this crucial piece of their response system.

Do Regular and Preventive Maintenance

Equipment built to public safety standards often comes with extended warranties that help underwrite the cost of repairing problems. Unlike consumer electronics, which occasionally find their way into emergency communications systems, public safety equipment is generally built to withstand years of routine use.

The equipment still needs maintenance, however. Both electronics and physical structures need to be inspected, tested for proper functioning, and adjusted. As much as modern radios are driven by embedded computers, they still have other internal components that occasionally need to be tuned. Likewise, physical components, such as towers, shelter HVAC (heating, ventilation, air conditioning), and power systems, need to be inspected and maintained. Just one lighting violation notice from the FAA due to a failed tower strobe can ruin a system manager's day!

Testing and maintenance records are important to keep. Prior work on equipment is always useful for technicians to have at hand and may be necessary for documenting equipment failure trends.

System infrastructure is tuned for optimal performance. Radio signal and line levels are adjusted for optimum performance, as are data network components. Records establishing a baseline for measurements and allowing tracking over time are invaluable for system maintenance. Some tuning measurements show seasonal shifts, while others show variance due to system load and component aging. Documentation of routine maintenance measurements is necessary for identifying and fixing problems. (For more information on policy, standards, and procedure maintenance, see Chapter 12).

One large jurisdiction with a P25 trunked radio system had to replace all of its new portable radios, numbering many thousands, not once, but twice. Technicians first found the radios unacceptably susceptible to other nearby portable transmissions, rendering them effectively deaf to the much weaker system signals from towers.

After the portables had been replaced with great effort, another design problem was found in the push-to-talk (PTT) switches, which weakened over time, causing multiple erroneous system requests each time the button was pressed. These problems were discovered through agency testing and documented to prove the problem.

Test at Least Monthly

Regular testing is important for assurance that the system will be available when needed. Schedule monthly tests, at least, to verify that system components are functioning as anticipated. The type and degree of testing should be established as a matter of policy and procedure.

End-user testing on a regular basis is a good means to assure that the system is operational. Technical testing needs to also be conducted to detect problems before they affect operations.

The Los Angeles Tactical Radio Communications System (LARTCS) is a joint effort of city, county, and state agencies in Los Angeles County. It is tested by user agencies twice a week. LARTCS connects together different radio systems through a gateway. See www.lartcs.org.

Maintain System Security

Unfortunately, system security is often overlooked. Both physical and electronic security of modern communications systems is important. While it's also time-consuming, agency and system managers need to provide the resources necessary for it to be done. Inspections, monitoring, and proactive measures are involved.

Physical security is the first bastion in protecting communications systems. All access control systems—from fences to lock keys to electronic access cards to active detection systems—require their own maintenance procedures.

Security is necessary for mission-critical systems.

Interagency SOPs should be set up to prevent breaches due to a single weak link. Nobody wants to be the weakest link! Use inspections and active monitoring to secure the systems.

Monitoring systems allow system managers to keep track of both physical access to communications facilities and logical access by, for example, remote computers for system configurations. Some components of voice radio systems, evermore computerized, can be reactively monitored by intrusion detection systems (IDS) and proactively secured by intrusion prevention systems (IPS). In effect, these systems watch for unusual activity and either provide notification and/or take action to mitigate impacts.

Intrusion detection and prevention systems can be used with central parts of digital radio systems.

Other proactive measures, such as encryption key management, are necessary to keep systems operating at expected levels of security. Key management is a serious and necessarily rigorous process for agencies using encrypted radio systems. We touch on it for both voice and data technologies, in the **Part 3 – Exploring the Technologies** later in this Guide.

As part of the critical infrastructure of our nation, it is essential that public safety communications systems are robust and secure. Responsibility for system security and infrastructure protection is not restricted to homeland security employees. Field responders on patrol or responding to calls can observe potential issues at radio sites or other communications facilities. Before your agency is faced with a disaster, put processes and procedures in place, and ensure expertise is available, to restore critical systems in a timely manner. The National Infrastructure Protection Plan (NIPP) provides a model for continuous improvement and directions to make systems better prepared to function when needed most. NIPP education and training are available and recommended for all agency staff, to improve the physical and electronic security of communications systems and the information they contain.[90]

90. See www.dhs.gov/files/programs/editorial_0827.shtm.

Prepare for System Changes

Finally, as much as you don't want to hear it, it's never too early to start preparing for system changes. System expansions of scope and depth are inevitable, as is the unending march of technology into the sea of obsolescence. Even harder to prepare for are regulatory changes that force changes to systems.

As another companion to the original *Law Enforcement Tech Guide*, SEARCH developed the *Law Enforcement Tech Guide on Information Technology Security: How to Assess Risk and Establish Effective Policies,* funded by the COPS Office (2006). See http://ric-zai-inc.com/ricphp?page=detail&id=COPS-P115.

Evaluate Potential System Upgrades

You prepared for system upgrades early in your project by documenting needs uncovered during early analysis and left unaddressed during implementation. Every project will have some share of nice-to-have features that went by the wayside as the project's scope, timeline, and budget were fixed. The oversight board can effectively keep participants actively engaged with a living, evolving system by recognizing these needs and working with participants to meet them over time.

Anticipate that unimplemented features of the chosen technology may become useful over time, as well. Vendors will have a natural interest in selling upgrades—initially minor and eventually major—that may address unmet needs. Use working committees actively to investigate upgrades, analyze their impacts, and make recommendations. For example, growing use of commercial wireless data networks subjects the agencies using them to rapid technology transitions—transitions that are uncommon with more slowly-evolving public safety technologies. Managers of interagency communications systems that use commercial services have to continuously analyze their vendors' technology life cycles.

Use working committees to actively investigate, analyze, and make recommendations on potential system upgrades.

Prepare for Regulatory Changes

In closing, most public safety radio users face regulatory changes. Large agencies and consortia can effectively handle the FCC regulatory process that governs the radio world, but it takes a significant commitment of time to stay on top of what, at times, seems to be a torrent of public notices, notices of public rulemaking, notices of inquiry, final reports, orders, and more.

Most agencies are more effective by working through their professional organizations, such as the International Association of Chiefs of Police (IACP), International Association of Fire Chiefs (IAFC), National Sheriffs' Association (NSA), National EMS Management Association (NEMSMA), the Association of Public-Safety Communications Officials – International (APCO), and the National Emergency Number Association (NENA).

Rely on professional organizations to help manage the effects of regulatory change.

The most significant regulatory issues are 800 MHz **rebanding**, release of **700 MHz spectrum**, and **narrowbanding** of public safety frequencies below 512 MHz. These changes affect pretty much all public safety radio users.

☐ Rebanding

Rebanding of 800 MHz is expected to cost $2.5 billion.

Rebanding of 800 MHz is necessary to move public safety users in that band away from the harmful interference they are receiving from commercial radio services. The move offers the opportunity to consolidate public safety spectrum, leading to improved management of systems and technological opportunities. The cost, estimated at $2.5 billion, is being borne by Nextel, whose facilities have interfered most with public safety operations.

Rebanding was to take place during a 3-year period ending by mid-2008. The FCC split the United States geographically into four zones known as waves. A "transition administrator" contacted licensees in affected portions of the 800 MHz band to plan and schedule the transition. The Public Safety and Homeland Security Bureau (PSHSB) of the FCC has extended the negotiation period for completion of the fourth wave border areas into 2012.

☐ New 700 MHz Spectrum

A good deal of new spectrum in the 700 MHz band for public safety became available in 2009 when incumbent television broadcasters were relocated. New, wider channels capable of higher speed data are available in this band. Existing 800 MHz systems in need of additional channels may look to add incremental 700 MHz channels as rebanding proceeds and equipment capable of the spread proliferates. (For more on 700 MHz Spectrum, as well as broadband, wideband, and LTE, see Chapters 16 and 17.)

☐ Narrowbanding

Narrowbanding will affect the majority of public safety agencies in the country.

The majority of public safety agencies in the country operate in VHF-high and lower UHF bands. This spectrum, between 150 and 512 MHz, has been the subject of intense debate for years among federal regulatory and public safety agencies. In an effort to make more efficient use of the bands, allowing more channels, the FCC released an order in late 2004.

The order set a deadline of January 1, 2011 for the manufacture and importation of equipment capable of wider band (25 kHz) channels. Applications for wider band channels were accepted until that 2011 deadline. All public safety voice operations between 150 and 512 MHz are to be moved to narrowband (12.5 kHz) channels by January 1, 2013.

Regulatory Resources

The 800 MHz rebanding is addressed in detail on the FCC website:
http://wireless.fcc.gov/publicsafety/800MHz/bandreconfiguration/index2.html

The FCC has designated a "transition administrator" to manage the tremendous change and cost associated with relocating 800 MHz users within the band. The transition administration website is:
www.800ta.org

The FCC's website on 700 MHz spectrum contains the most up-to-date information on efforts across the country to put this spectrum to use:
http://wireless.fcc.gov/publicsafety/700MHz

Efforts to "refarm" spectrum use below 512 MHz have been under way since 1992. The most recent regulations require reductions in the amount of spectral space used, referred to as "narrowbanding." See the FCC website:
http://wireless.fcc.gov/services/plmrs/refarming

CHAPTER 15

Measuring Interoperability

What: Measuring refers to a *process* for subjectively assessing communications interoperability across five accepted dimensions.

Why: Plot your current position and heading, with mid-course corrections, to verify that you are on track to achieving interoperability.

Who: The governing body of the interagency initiative or project is in the best position to complete the assessment itself, or to direct a more thorough assessment across participating agencies.

When: Measure the state of interoperability early and repeat the assessment at least annually.

Interoperability is a difficult quality to measure. Forgetting the fact that the term has come to be used in reference to everything from fire hose couplings to web-based software services, it's an elusive capacity that only truly shows itself in practice, not as some sort of static state of being. It is a necessary capacity allowing public safety agencies to work together to achieve their respective missions in protecting the public.

Interoperability isn't a destination; it's a waypoint.

Interoperability isn't a destination; it's a waypoint. Your agency's destination may be different from the next, but all rely on an ability to communicate with others. The "ability" isn't always necessarily used, so the mere capacity to communicate doesn't tell us whether it's put to beneficial use. Our measures of current position and course have to take into account not only the technical capacity, but also its practical application to prevent, deter, respond to, and recover from the effects of hazards of all types.

The agencies involved in your communications interoperability efforts will have excellent reasons to frequently measure interoperability over time. This chapter offers a subjective assessment process to help those involved in your initiative show progress on the route that has been charted.

Communications interoperability is a complex, but important, issue to measure. It will become more complex over time.

Why Measure Interoperability?

You get what you measure.

Any effort to improve the capabilities or performance of organizations needs to establish a baseline to assess progress and regularly reassess it to steer efforts toward the desired destination. Measures of communications interoperability have to be carefully chosen and defined to ensure that what is being assessed is what is desired. ***You get what you measure.***

Measures communicate.

The process of measuring interoperability offers benefits. It helps to focus effort on the achievable, rather than simplistic ideals, by establishing understandable, observable objectives. It encourages joint ownership of both the objectives and the progress in meeting them. It provides a tool for accountability. Most of all, it communicates in a language of objectives that, even if imperfect, can be common among stakeholders.

Measures reflect objectives on course to achieving goals.

The measures chosen must accurately and adequately reflect the desired goal, being accepted both as relevant and measurable. Recognize that measures, objectives, and goals are progressive. Achieving interoperability between public safety communications systems is only a step to achieving the greater goal of *interoperations*. Ultimately, the measure of interagency communications is its yeoman service, unobtrusively and effectively supporting public safety responders working across disciplines, jurisdictions, and levels of government to serve the public.

Cautious Measures

A strong conviction that something must be done is the parent of many bad measures.

—*Daniel Webster*

A point of note before proceeding: Interoperability has not only become an important rallying cry, but has also come to mean widely different things to different people. To some, it is the willingness of agencies to work together. To others, it is merely having compatible technologies. To most, it is a term that has grown in importance following national tragedies and responder cries for better communications.

The basic measures of communications interoperability addressed in this chapter have been carefully crafted by the public safety response community. While basic, they are not simplistic, nor are they particularly simple to achieve. They are, however, the common elements that are broadly recognized as key to this elusive quality called *interoperability*.

Figure 15-1: SAFECOM Baseline Survey Elements (2006)

Interoperability Continuum Element	Baseline Survey Sub-element
Governance	Leadership Decision-making Groups Agreements Interoperability Funding Strategic Planning
Standard Operating Procedures	Policy, Practices, and Procedures Command and Control
Technology	Approaches Implementation Maintenance and Support
Training and Exercises	Operator Training Exercises
Usage	Frequency of Use and Familiarity

The Interoperability Baseline Scorecard

Agencies have identified the need for a basic, yet relevant, means of assessing their communications interoperability. Drawing on the results of SAFECOM's National Interoperability Baseline Survey,[91] a simple process is offered here for marking the current state of your initiative and assessing its progress over time.

SAFECOM's National Interoperability Baseline Survey

In 2006, SAFECOM initiated a project to define an interoperability baseline. The multi-phase process first sought to define how the level of interoperability in an agency or a region can be assessed. The goal was to provide the means to understand the current state of interoperability. A practitioner working group was established to collaborate with staff and contractors preparing the survey.[92]

Previous studies of communications interoperability have narrowly focused on the issue. The baseline survey uses the five dimensions of interoperability introduced in the *Interoperability Continuum* to get more deeply at the root of key interagency communications factors (see Figure 15-1). Through development of a "straw man" measurement tool and its refinement by four focus groups held across the United States, 13 measurable sub-elements of these dimensions were chosen for assessing interoperability.

91. For information on the National Baseline Survey, see www.safecomprogram.gov/baseline/Default.aspx.

92. The original author of this Guide was a member of the SAFECOM Advisory and the Baseline Working Groups.

Descriptive measures of each sub-element were developed for assessing whether an organization was in an early, moderate, or full stage of development for communications interoperability. Additional measures were developed to identify advanced stages of development as well. This measurement tool arising from the original *Interoperability Continuum*, consisting of the elements, their sub-elements, and the descriptive measures for each stage of development, was the basis for the baseline survey matrix.

Conduct a Self-assessment

You may be preparing for a multiagency initiative to improve interoperability, in the midst of a project as we've discussed throughout this Guide, or even proceeding to sustain a long-term effort. In situations like these and others, a baseline is always useful. A baseline—and the earlier identified the better—establishes a multidimensional picture of where the agency, project, or initiative is at that point in time. Subsequent self-assessments can be used to determine if progress is being made across the continuum. Annual assessments as part of a continuous improvement program can help link progress with programs.

The Interoperability Self-assessment Scorecard

The *Interoperability Self-assessment Scorecard* in Appendix D is a simplified form of SAFECOM's baseline survey tool (an example of which is provided as Figure 15-2). This self-assessment is useful with small and large groups alike. It can serve as an icebreaker with new groups or be used to apply SAFECOM's baseline process formally to a particular initiative. It's also easily replicable, meaning that it can be used over time to gauge progress.

The National Baseline Survey presented one or more questions for each of the 13 sub-elements and asked respondents to indicate separately across disciplines, jurisdictions, and levels of government whether one of four statements—corresponding to early, moderate, full, or advanced stages of development—best described their situation.

The *Scorecard* uses the survey tool's questions and measures, but collects a singular assessment of each sub-element across disciplines and jurisdictions in a matrix for presentation. It presents the four statements and asks for a subjective assessment of the current stage of development across partners or project participants using further prompts both from the assessment methodology and baseline measurement tool.

Figure 15-2: Interoperability Self-assessment Scorecard Example

EXAMPLE	**Consider the question and how this measure varies across organizations, then choose one of these stages of development.**	
Governance: Strategic Planning ***Strategic Planning*** *How would you best describe the planning efforts to make decisions, take actions, and create processes that ensure interoperability?* — No interoperability strategic plan in place; some preliminary planning may have begun — Strategic planning process in place and plan under development — Strategic plan in place and accepted by all participating organizations — Strategic plans reviewed annually and after system upgrades and events that test your organization's capabilities	☐	**Early Development** No interoperability strategic plan or strategy in place
	☐	**Moderate Development** Strategic planning process in place and plan under development
	☐	**Full Development** Formal strategic plan in place and accepted by all participating stakeholders
	☐	**Advanced Development** Institutionalized processes to review strategic plans on an annual basis and after significant events or upgrades

The self-assessment is necessarily subjective. While you may (and should!) strive to be objective in assessing your agency, jurisdiction, or region's communications interoperability, it's still based on personal observations and conclusions. Its primary importance is in establishing a baseline against which subsequent, equivalent assessments can be compared and in communicating objective elements of success in achieving communications interoperability.

Using the Self-assessment Scorecard

Even a subjective self-assessment can provide a tangible reference of where you currently are and guidance on where you are headed. Whether conducted as a structured poll or presented interactively to a group, keep in mind that this is a subjective survey of a limited audience, not a scientifically applied survey to a carefully selected sample. The results are useful for putting a stake in the stand and seeking consensus on needed areas of work.

Figure 15-3: Interoperability Self-assessment Scorecard Example

		Stage of Development			
Element	**Subelement**	**Early**	**Moderate**	**Full**	**Advanced**
Governance	Leadership		✔✔✔	✔✔✔✔✔	✔✔
	Decision-making Groups	✔	✔✔✔✔✔	✔✔✔	✔
	Agreements	✔✔✔✔✔✔	✔✔✔	✔	
	Interoperability Funding	✔✔✔✔✔✔✔✔✔✔	✔		
	Strategic Planning	✔✔✔✔✔✔	✔✔	✔✔	
Standard Operating Procedures	Policy, Practices, and Procedures	✔✔✔✔	✔✔✔✔	✔✔	
	Command and Control	✔✔✔	✔✔✔	✔✔✔	✔
Technology	Approaches	✔✔✔✔✔	✔✔✔	✔	✔
	Implementation	✔✔✔✔	✔✔✔✔✔	✔	
	Maintenance and Support	✔✔✔✔✔✔	✔✔	✔✔	
Training and Exercises	Operator Training	✔✔✔✔✔✔✔	✔✔	✔	
	Exercises	✔✔✔✔	✔✔✔✔✔	✔	
Usage	Frequency of Use and Familiarity	✔✔✔✔	✔✔✔✔	✔✔	

Step 1
Find a Suitable Venue

Use the *Scorecard* as either a standalone survey distributed to your project committees, system oversight board, or any other group with a shared interest in communications interoperability. Or during a meeting, present the sub-elements interactively. Ask the group through a showing of hands or something more imaginative how their organization rates the current state of affairs.

Step 2
Collect and Compile Responses

Collect and compile the results in some graphic format to depict the distribution of responses for "analysis." Another *Scorecard*, as shown in Figure 15-3, serves well to collect all the responses. Whether through a distributed survey or interactive poll, again remember that the results are simply a subjective assessment of a limited audience.

In this hypothetical example, a 10-person Steering Committee of a communications interoperability project is asked to evaluate their organizations' interoperability using the *Scorecard*. Responses are simply tabulated using check marks. On the *Scorecard*, the stage of development, early through advanced, is described specifically for each sub-element using descriptions taken from the SAFECOM *Interoperability Continuum* measurement tool.

Step 3
Analyze the Results

There's not much "analysis" to do, but watch out for a couple of potentially odd results.

First, without getting into statistical theory, any survey or poll of more than just a few people is going to show a distribution of responses. If the audience is at all diverse (most likely so with interoperability initiatives!), there will be a response or two well outside the others. While there's no wrong answer in this survey, it's unlikely that a single agency is much more or less interoperable than its neighbors. For example in the *Scorecard* above, "Approaches" drew one response far from the median. For purposes of finding some consensus measure, it can be ignored.

Second, a flat distribution of something, as shown under "Command and Control" above, indicates there were either multiple interpretations of the question, differences between represented disciplines, or other widely varying perceptions. In any case, it bears further investigation. The discrepancy may indicate a particularly thorny dimension of interoperability between the participants that needs to be addressed.

Step 4
Present the Results

Carefully present the *Scorecard* results. They can be misinterpreted or misconstrued if presented outside the context of the questions asked and measures used, so explain the results in terms of the stages of development. For example, the "Frequency of Use and Familiarity" results tabulated in Figure 15-3, examined in comparison to development definitions included with the *Scorecard* (see Figure 15-4 on page 262), are fairly clear. They could be reasonably understood to suggest respondents collectively concluded that the agencies use solutions during planned events and somewhat regularly during emergencies, but rarely for routine communications. Without the context of these definitions, the stages of development may be understood too broadly to be useful.

Figure 15-4: Interoperability Self-assessment Scorecard Development Definitions

Usage: Frequency of Use and Familiarity

Early Development	Moderate Development	Full Development	Advanced Development
First responders seldom use solutions unless advanced planning is possible (e.g., special event)	First responders use solutions regularly for emergency events, and in a limited fashion for day-to-day communications	First responders use solutions regularly and easily for all day-to-day, task force, and mutual aid events	Regular use of seamless solutions has expanded to include state, federal, and private responders

Performance Measures

Performance measurement, in simplest terms, is the comparison of actual levels of performance to pre-established target levels of performance. To be effective, performance must be linked to the organizational strategic plan.

— *The Performance-based Management Handbook, U.S. Department of Energy*

Increasingly, effective management of public safety agencies requires the use of a performance measurement program rich in strategy and solid in application. Well implemented, such a program ensures, among other things, that projects undertaken are aligned with organizational goals and objectives, provide tangible improvements, manage factors associated with success and failure, are replicable, and through all demonstrate a fair return on investment. Ultimately, performance measures are the only legitimate means of evaluating organizational goals and objectives.[93]

While the *Scorecard* described above can be useful in sketching a baseline for your interoperability initiative and charting its progress, it is neither a fair nor adequate measure of performance. Until the introduction of the *Interoperability Continuum* and the National Emergency Communications Plan (NECP), the absence of performance goals and measures presented a national challenge in achieving interoperability. (See "GAO Congressional Testimony" on page 264.) As a result, the OEC published the *Communications Interoperability Performance Measurement Guide* in April 2011.[94]

This guide goes into more detail than it is practical to discuss here. It effectively addresses understanding, developing, and using performance measures that focus on response-level emergency communications, and integrates these performance measures across governments, the interoperability continuum, the NECP, and other initiatives.

93. As another companion to the original *Tech Guide*, SEARCH developed the *Law Enforcement Tech Guide for Creating Performance Measures that Work: A Guide for Executives and Managers,* funded by the COPS Office (2006). See http://ric-zai-inc.com/ric.php?page=detail&id=COPS-P120.

94. *The Communications Interoperability Performance Measurement Guide* is available at www.safecomprogram.gov/SiteCollectionDocuments/OECPerformanceMeasurementGuide.pdf.

NECP Goals:

Goal 1–By 2010, 90 percent of all high-risk urban areas designated within the Urban Areas Security Initiative (UASI) are able to demonstrate response-level emergency communications within one hour for routine events involving multiple jurisdictions and agencies.

Goal 2–By 2011, 75 percent of non-UASI jurisdictions are able to demonstrate response-level emergency communications within one hour for routine events involving multiple jurisdictions and agencies.[95]

Goal 3–By 2013, 75 percent of all jurisdictions are able to demonstrate response-level emergency communications within three hours, in the event of a significant incident as outlined in national planning scenarios.

Measuring Effects, Not Capabilities

In and of itself, interoperability is unlikely to be a strategic goal of agencies whose missions revolve around protecting public safety. Interagency communications is certainly a key resource in many operations, but it is just part of the interagency processes through which mutual services are delivered. The outcomes and impacts of those processes—not some technical capacity to communicate—are the appropriate subjects of performance indicators.

Communications interoperability is more than the mere *capability* to communicate across agencies. In the most fundamental sense, it is the absence of communications impediments in interagency operations. Inasmuch as too much communications can actually interfere with operations at times, and *intra*-agency communications needs typically far outweigh those between agencies, interoperability is a low performance indicator for some processes. It's not hard to imagine that high performance indicators of some interagency operations may necessarily be very limited (or highly controlled) interagency communications.

This is not to say that communications interoperability is unimportant. Hardly! Interoperability performance measures are inseparable from measures of mutual business process performance between agencies. Communications interoperability is the condition, *ipso facto*, that needed resources are available. What's needed can only be determined through rigorous definition of **business processes** (the right things being done) and **performance measures** for those processes (things being done right).

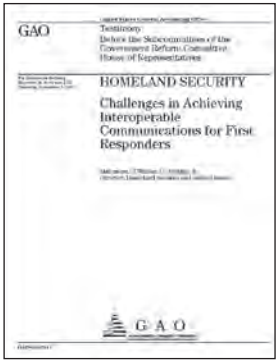
Interoperability performance measures are inseparable from measures of mutual business processes.

95. The State/Local and Tribal Response Level Communications Tools (RLCTs) were developed to provide state, urban, local, and tribal practitioners with an after-action reporting capability to independently and regularly assess response-level emergency communications following planned events and real incidents involving multiple jurisdictions and agencies. These tools are available at www.publicsafetytools.info.

☐ An Example

Radio gateways play an important role in linking separate networks. They are notorious, however, for causing problems when misused—a very real potential with many implementations. By linking two channels, they potentially double the amount of traffic on each, tripling it with three channels, and so on. If the mere presence of a gateway is factored as a measure of interoperability, the measure may neglect the more important factor of *how* the gateway is used: That is, whether in fact it actually improves or reduces communications capabilities and operational performance.

GAO Congressional Testimony



In 2003 Congressional testimony, the General Accounting Office (GAO—now Government Accountability Office) identified performance goals and technical standards as the second of three most pressing challenges in achieving interoperability, following definition of what interoperability is and preceding definition of intergovernmental roles.

"When the interoperability problem has been sufficiently defined and bounded, the next challenge will be to develop national interoperability performance goals and technical standards that balance consistency with the need for flexibility in adapting them to state and regional needs and circumstances."

—U.S. General Accounting Office, *Homeland Security: Challenges in Achieving Interoperable Communications for First Responders,* GAO 04-231T (Washington, D.C.: Nov. 6, 2003).
See www.gao.gov/new.items/d04231t.pdf.

Performance Measurement Improves Communications

Given our topic, it's ironic that a side benefit of a well-implemented performance measurement program is improved communications within organizations, as well as with external stakeholders. It improves communications by clearly relating performance objectives to service goals and explicitly stating indicators of success. A system of systems that improves interagency communications will actually flourish through agency performance management programs that include measures of interagency *operations*. It will do so because key business processes (and performance indicators) will have been defined, and thus more easily communicated.

If this all sounds reminiscent of our discussion of needs analysis in Chapter 6, it should. The first step in analyzing needs for your project was defining interagency business processes and the final product was a business process baseline report. Not only does a thorough understanding of business processes provide the framework for technology projects, it's also the heart of performance measurement.

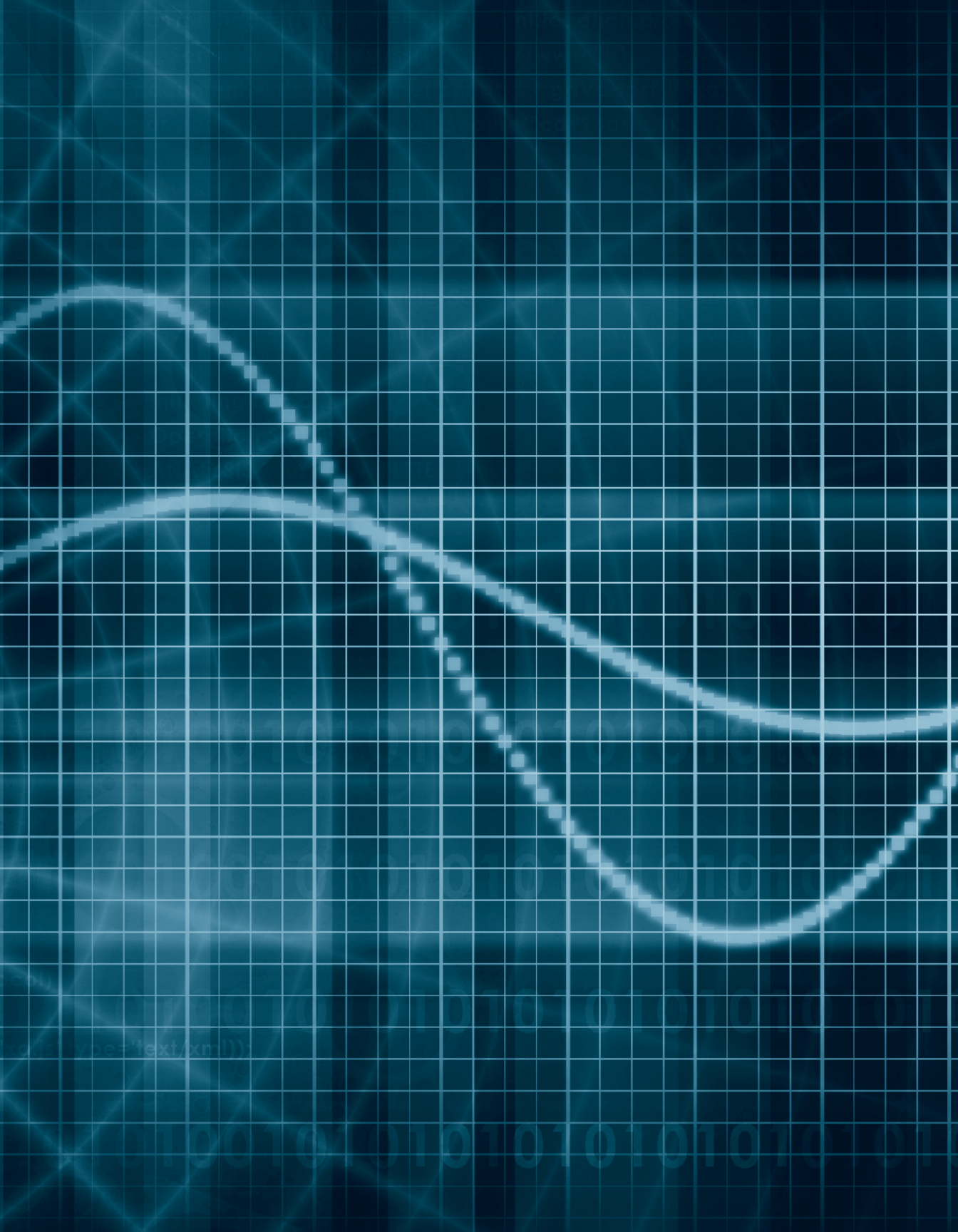
Conclusion

The bottom line is this: **Performance measurement is based on business needs, not technological capabilities.** It is impossible to measure the performance of technology independent of the performance of the business processes it supports. The most highly featured system cannot be shown to benefit an agency or multiple agencies that don't actively manage their own business process performance.

Communications interoperability projects will be subjected to required proofs of performance more and more in the coming years. The scope, cost, and intended impact of these projects is just too large to proceed on broad emotional appeals. The public, elected officials, and funding agencies all demand accountability.

The charge for agency administrators and project managers will be to show the needed performance benefit of improved interagency communications and why technology is needed to accomplish it.

Part 3: Exploring the Technologies



CHAPTER 16

Voice Communications

Guideposts: Exploring the Technologies

THE FINAL PART OF THIS GUIDE INTRODUCES BASIC TECHNOLOGIES used for public safety communications, generally, and interagency communications, more specifically. In this chapter, we start with background on the basic technologies used for voice communications and then delve more deeply into their application for interoperability.

We'll cover:

- Understanding the Technologies
  - FCC Classification of Radio Systems
  - Analog and Digital Radio Technologies
  - Conventional and Trunked Radio Systems
  - Communications in Tunnels and Buildings
  - Satellite Communications
  - VoIP in Voice Systems
- Approaches to Interoperability
  - Technology Approach: Swap Radios
  - Technology Approach: Gateways
  - Technology Approach: Shared Channels
  - Technology Approach: Shared Systems
- Security
  - Advanced Radio Features for Physical Security
  - Encryption and Key Management

In Chapter 17, we address data communications, as it may be used for everything from simple text to live video.

Note: As of the printing of this guide, changes have already been observed in the field of voice communications. Be sure to refer to information produced on the First Responder Network Authority (FirstNet) and the National Telecommunications and Information Administration (NTIA). See **http://www.ntia.doc.gov/category/firstnet**.

Have faith. Someone is thinking about the future.

Any radio or mobile data system will only perform as well as it is funded and engineered.

—Steve Proctor, Executive Director, Utah Communications Agency Network

Many user devices interact through several applications, across various technologies. If it seems terribly confusing, take heart. Your responsibilities probably take your time and available attentions elsewhere on a daily basis. Your responsibility to manage an agency, a division, or this particular interoperability project probably leaves little time to delve this deeply into technology.

Have faith that there are technologists who understand where you are today and what technologies are likely to enable your operations tomorrow. Your own job more likely entails understanding the public safety business, getting and using funding effectively to improve operations, and figuring out how you're going to work with partners in response.

SAFECOM Library

The SAFECOM online library is a prime source for technical information about voice communications systems. It includes documents from multiple sources, including the past Public Safety Wireless Network (PSWN) Program. See www.safecomprogram.gov/library/Items.aspx?CATID=Technology Solutions and Standards.

Understanding the Technologies

Public safety communications technology parallels consumer and other commercial technologies. As more digital communications are used, voice becomes more indistinguishable as the "payload" over much of the networks connecting senders and receivers of information. It has unique features that shape how it's moved from the analog world of sound, handled over digital transmission systems, and then converted back to sound. However, in most ways it can be transported and stored in digital form just like more traditional data.

While voice and data communications for public safety services have long been conducted over both wired and wireless links, we focus here mostly on the latter. It's there that the greatest communications interoperability challenges have occurred for responders (although advanced radio systems increasingly include many wired components at their cores, just as voice and data are increasingly intertwined in emergency response communications).

FCC Classification of Radio Systems

Before we look at the primary voice radio technologies, let's pause to clarify some terminology and look at FCC classifications of radio systems. We should note that a standard definition of "radio system" does not exist. This leaves each agency free to define their system, which can ultimately contribute to interoperability issues.

The FCC uses specific terms to distinguish radio technologies and their uses. The term *type* is used to distinguish different fundamental technologies, while *services* distinguish between different applications of the technology.

The FCC distinguishes radio *types* and *services*.

The term *type acceptance* is commonly used in the radio world. It refers to the FCC's formal process of evaluating and approving technologies. Individual manufacturer radio models must receive FCC-type acceptance before they can be made commercially available. It's not uncommon to hear manufacturer representatives speak of new models and note they are awaiting type acceptance before they will be mass-manufactured and sold.

The FCC classifies most public safety radio systems as *private radio.*

Several *radio services* are used by public safety agencies, including:

- Broadcast
- Commercial
- Specialized mobile
- Aeronautic
- Maritime
- Amateur
- Unlicensed
- Land mobile

Traditional dispatch, car-to-car, and field communications used by public safety is *land mobile radio* (LMR). This term is commonly used by industry and in regulations in reference to terrestrial radio services to support mobile users. Portable and car radios are both classified as "mobile" at this level of discussion.

More than 300 agencies in South Carolina use the Palmetto 800 System, an 800 MHz system shared with power utility companies. For further information, see: http://cio.sc.gov/councilscommittees/palmetto800/.

While several of the radio services listed above are probably recognizable to readers, others may be confusing. Most public safety radio networks are regulated by the FCC as *private radio* systems. Where common carrier systems are made commercially available for general public use, those built and operated for private use are considered private systems. In this case, "private" refers to how they're used, rather than owned.

Many commercial industries have their own private radio systems. A few are actually shared with public safety agencies, but the vast majority of police, fire, and EMS voice radio communications takes place over systems owned and operated by the agencies themselves. Most of these systems require FCC licensing. Unlicensed radio technologies, such as those that might be used for wireless local area networks (WLANs), are regulated separately.

Whether licensed or unlicensed, private or common carrier, radio technologies are broadly subject to FCC regulations. Rely on your radio technicians, vendor representatives, frequency coordinators, and professional associations to help you sort out details if you intend to be heavily involved in radio technology.

Analog and Digital Radio Technologies

For the first century of radio, analog radio technologies predominated. Those technologies include *amplitude modulated* (AM) and *frequency modulated* (FM) radios that we're all familiar with from broadcast radio services. Others exist, but all analog technologies are based on use of audio tones (frequencies) being superimposed on radio frequencies (RF) in a standardized manner.

Audio frequencies, such as those delivered electronically by radio microphones, are mixed with RF within analog radio circuitry, further amplified, and then transmitted. At distant receivers, the audio is extracted electronically in more or less the reverse manner. Data can be transmitted much like voice over analog systems by encoding bits using different audio tones and other techniques of shaping the transmitted RF signal.

Public safety frequency bands for voice communications are typically described in megahertz, while channel bandwidths are described in kilohertz.

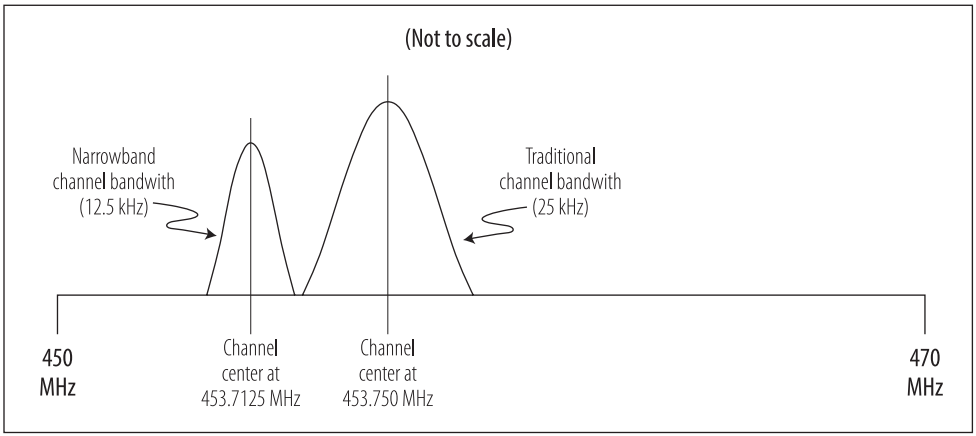
☐ Channel Bandwidth

Frequency modulation (FM) is by far the most common analog radio mode today. It is also the compatibility or legacy mode for digital radios. However, transmitters and receivers not only have to use common means of putting information on the RF signal (i.e., modulating it), they also have to use compatible channel widths and operate in the same frequency band, such as VHF, UHF, 700, or 800 MHz.

Frequency bands for common public safety voice purposes are typically described in millions of radio wave cycles per second (megahertz is abbreviated as MHz) (Figure 16-1 on page 275). They are occupied by channels of a certain *bandwidth*. That is, they take up a specific amount of the frequency band.

Channel bandwidths are described in thousands of cycles per second (kilohertz is abbreviated as kHz). A channel is a slice of some part of the radio frequency spectrum. That is, we talk about a traditional 25 kHz voice channel in the 450 MHz public safety frequency band. A traditional voice channel in that band has been allotted 25 kHz of RF spectrum.

Figure 16-1: Public Safety UHF Frequency Band, 450-470 MHz



☐ Narrowband Channels

Narrowbanding, as discussed in Chapter 14 (page 250), is an FCC regulatory effort that affects all analog radio users. Its goal is to reduce the amount of RF spectrum occupied by a single channel to increase the number of channels that can fit in a given band. This is not the first time the FCC has split channels for this purpose and we can expect it to happen again.

The FM radio channel has existed for decades as nominally 25 kHz in width. We say "nominally" because channel width is more an absolute under regulations than under the laws of physics. It actually varies in width according to transmitter adjustments and characteristics of the audio being carried. In addition, the transmitted power isn't all contained within the defined channel; a progressively smaller fraction exists farther and farther away from the channel center.

The FCC requires that public safety operations move to 12.5 kHz channels or the equivalent by January 1, 2013.

FCC rules mandate that all public safety voice operations between 150 and 512 MHz move to narrowband (12.5 kHz) channels by January 1, 2013. Technically, the requirement is that a channel can occupy no more than 12.5 kHz or the effective equivalent. This last clause can be a bit confusing. There are proprietary techniques to interweave two separate conversations, both using the whole 25 kHz, but splitting use of the channel second by second. Most commonly, the narrowband channel will be used wholly for a single communications path.

One net effect of this transition is that narrowband analog transmitters will have less spectral space to put RF energy, thus reducing the power and range of an analog channel relative to the wider band channel. Just how much is the subject of debate, but recognize that the range of a narrowband transmitter will be less than that of its wider band cousin.

While digital uses of these radio bands are similarly affected, existing digital technologies already use 12.5 kHz channels or allow multiple voice conversations to occur within a traditional 25 kHz channel. Narrowbanding is thus leading to wider adoption of digital techniques.

☐ Digital Radio

A vocoder converts analog sound to digital bits.

Digital radios use many of the same components as their analog relatives. For voice radio purposes, microphone audio frequencies are first converted into bits by the voice *encoder* or *vocoder*. This is a particularly important part of the digital radio system; not all vocoders are created equally. For public safety purposes, great work has gone into testing and choosing vocoders that efficiently produce a digital stream to make most use of the radio channel.

The P25 vocoder standard carefully balances efficiency, robustness, and fidelity.

The process of creating digitized audio, transmitting it over the largely inhospitable airwaves, and decoding it on receivers is fraught with danger for the lowly voice bit. Project 25 (P25),[96] which produced the national standard for public safety digital voice radio systems, took on the challenge. It undertook a significant effort to find a vocoder sufficiently efficient, yet producing resiliently encoded audio for the most critical missions, in some of the most difficult radio environments. The Project 25 vocoder standard was selected as a careful balance of efficiency, robustness, and fidelity.

Using digital radios in the presence of background noise can cause distorted audio. Testing confirmed the distortion was so severe in many situations that transmissions were unintelligible. In response, an Audio Performance Working Group was created to work on this important issue. In 2009, manufacturers began shipping radios with an updated P25 vocoder. The updated vocoder has significantly improved distortion levels, but has not solved the problem.[97]

96. Initiated by the Association of Public-Safety Communications Officials (APCO) International, in cooperation with the National Association of State Telecommunications Directors (NASTD) and with support of other public safety organizations like the International Association of Chiefs of Police (IACP), Project 25 received its name following APCO's tradition of numbering its broad initiatives to affect the public safety communications world. P25, as it is also commonly known, is the association's best-known project. The specifications have been codified by standards development organizations. For further information, see www.project25.org.

97. D.J. Atkinson, "Update on Public Safety Communications Intelligibility in High Background Noise," presentation, March 2009, www.pscr.gov/about_pscr/highlights/iwce_2010/iwce_2010_audio_20100310.pdf.

Manufacturers are also introducing interim solutions that, when combined with the new vocoders, reduce the distortion even more. These solutions involve filtering techniques using microphones. An example involves installing dual microphones, one on the front to receive the audio and one on the back to cancel out any background noise. If the only microphones used were in the portable radio or on a shoulder microphone, that could be acceptable; however, when a firefighter is wearing a facemask, the acoustic coupling in the facemask causes a problem. To solve this problem, manufacturers are working on building filtering devices into the facemasks and using bone conduction microphone technologies.

While creating the ideal vocoder is still the desired mechanical solution, training personnel in radio use best practices in high background-noise environments can be valuable. There may not be agreement on a specific solution at this point; however, there is agreement and cooperation between public safety and industry to find multiple solutions that will address the wide variety of scenarios faced by field responders.[98]

Radio transmissions are weakened over distance and by the environment.

Digital radio standards for public safety don't stop at speech encoding, however. As a matter of fact, the vocoder is just a small part of the technology that takes audio, encodes it, packages it up, inserts it aboard the radio channel train, and assures it can be unpackaged successfully on the other end.

Another key piece of the Project 25 standard is its *Common Air Interface* (CAI), which provides the standardized means for receiving radios to recognize what is coming over the airwaves and extract an intelligible signal. Any digital receiver has to know how to decode the audio bit stream once received and passed to internal microprocessors, and then convert it back to audio frequencies that can be heard through speakers. That's not all, though. Receiving radios also have to know when and where a package of bits begins and ends, how to deal with inevitably missing or erroneous bits, how to recognize other embedded codes, and more. Project 25's CAI is the standard for how that's done with public safety digital voice radios.

The P25 Common Air Interface is the public safety standard for digital, RF transmissions.

Standards are absolutely essential for interoperability of radio systems. Congress directed the creation of the P25 Compliance Assessment Program (CAP) to ensure that when a vendor advertises equipment as "P25-compliant" it is, in fact, P25-compliant. The intent of the program is to provide vendors with a way to test their products, and ultimately to help public safety officials make better purchasing decisions. The first order of business for the CAP is the CAI.[99]

98. For sample audio demonstrating the difference in distortion before and after solutions are applied, see www.pscr.gov/about_pscr/highlights/iwce_2010/iwce_2010_audio_20100310.pdf.

99. For more information on the P25 CAP, see www.safecomprogram.gov/currentprojects/project25cap/Default.aspx.

☐ The Radio Environment – Analog

Once transmitted, all radio waves are subjected to the same environmental effects regardless of their payload. The laws of physics aren't particularly concerned with whether they're bearing analog or digitally encoded information.

It's a hostile environment. Received radio signals may be millions and millions of times weaker than they were at their source. Not only do signals diminish geometrically as a function of distance, they also are weakened or *attenuated* by the environment over and through which they pass. Manmade and natural obstructions both tend to absorb radio waves. Similarly, each time a radio wave is reflected or diffracted (which is often!), it scatters and loses a bit more energy. Add to this the additional challenges imposed by relatively rapidly moving transmitters and receivers and it's nothing short of fundamental magic that any intelligence can be extracted from distant transmissions!

Anyone who has listened to an FM broadcast recognizes the sound of a station fading in and out. If you've listened carefully in areas where FM broadcast stations overlap on the same frequency, you've also heard the effects of two roughly equal signals competing in your receiver. "Roughly" in the radio world is measured in factors of tens and hundreds. A signal that is 100 times or stronger than competing signals will generally be the only one heard on a channel. In the radio environment, signals can vary by a factor of a hundred within the distance of a few feet.

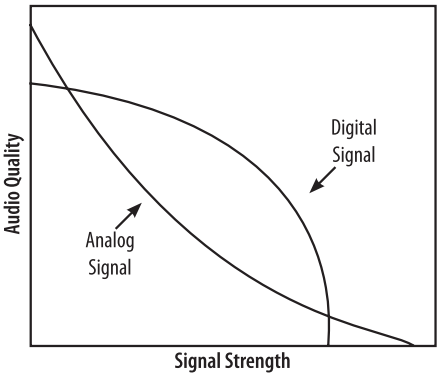
Overlapping radio signals cause interference in receivers.

FM has something called the *capture effect* whereby once a receiver is locked on to a given signal, it rejects a competing one up to a point. As the new signal becomes increasingly stronger, the receiver finally gives up on the first and locks onto the second. In between, distorted and mixed audio is heard. Portable and mobile radio users of two-way FM channels quickly learn to recognize the signs of one user "walking on" another through overlapping transmissions.

☐ The Radio Environment – Digital

Digital radio technologies designed for public safety use error correction techniques to recover intelligible audio from signals that are battered about by the environment and other radio users. *Forward error correction* (FEC) techniques are used to allow a receiver to recreate a damaged signal from, in effect, redundant parts of the digital stream. Additional signal information takes up part of the digital channel for FEC purposes.

Figure 16-2: Recovered Audio Quality by Signal Type



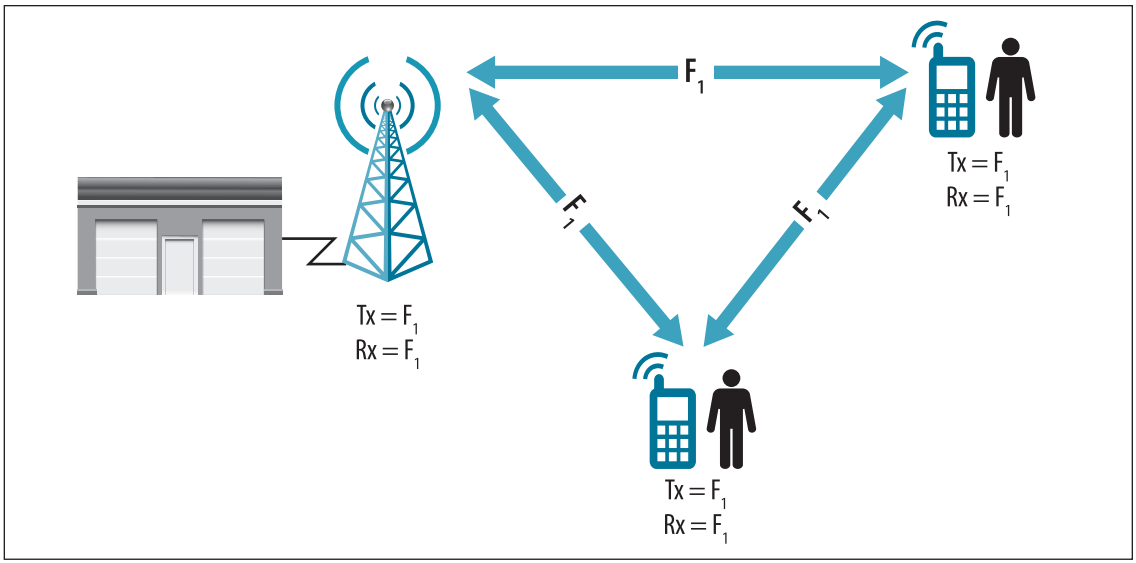
The term *bit error rate* (BER) is used to describe the percentage of received bits in a digital stream that are "broken." While public safety radio technologies can recover nearly original audio with BERs in the vicinity of 2 percent, recovered audio starts to degrade as error rates increase.[100] Anyone who has used a cellular telephone has noticed the effect of weak digital signals on caller voice intelligibility. At some point the BER becomes too high for digital signal processors to recover accurate audio from the digital stream, leading the receiver to shut off digital-to-audio conversion rather than pushing noise to its speaker.

While the human ear and brain has a remarkable ability to recover intelligent audio in the presence of relatively high noise levels, digital radio receivers are more limited. At some point they have to stop trying lest they start making up sounds that weren't originally there. By comparison, intelligible audio can be discerned by the human ear through an FM or other analog receiver at a lower signal level than a digital receiver can use. Refer to Figure 16-2. On the other hand, a digital receiver can recreate the identical audio signal that was sent, while the received analog signal gains increasing background noise as it gets weaker.

Let's move on to the different types of systems that put analog and digital radio technologies to work.

100. John M. Vanderau, *Delivered Audio Quality Measurements on Project 25 Land Mobile Radios*, NTIA Report 99-358, Washington, D.C.: U.S. Department of Commerce, Institute for Telecommunications Science, 1998. A BER of 2 percent corresponds to a Delivered Audio Quality (DAQ) measure of 3.4. See www.its.bldrdoc.gov/pub/ntia-rpt/99-358/.

Figure 16-3: Simplex Radio Example



Conventional and Trunked Radio Systems

There are two broad categories of radio systems used for voice communications today: conventional and trunked. In order to understand the difference, it's useful to first understand a few basic system principles and common building blocks.

☐ Building Blocks – Simplex Communications

Land mobile radio systems are commonly designed to allow one party in a conversation to talk while others listen. By contrast, telephone systems throughout the years have been designed so both parties may speak simultaneously. Voice radio protocols in public safety have evolved around the fact that only one speaker has access to a channel at a time.

The common term for this form of communications is *simplex*. In radio usage, the term carries further meaning. Simplex radio channels carry conversations conducted on a single frequency where participant radios transmit (Tx) and receive (Rx) on the same frequency. In Figure 16-3, "Frequency 1" (F_1) is used for all transmissions.

The radio depicted at the tower is referred to as a *fixed-base station*, whether it is closely or remotely attached to agency facilities. The base station could be placed on a mountaintop far from dispatch facilities, for example, and controlled remotely.

This approach to radio communications works well and is the simplest, most resilient form of coverage when all radio users are within range of one another. It becomes problematic, though, when radio end users move out of range of each other.

In all two-way voice systems, from the simplest to most complex, radio coverage is, well, a two-way street. It's relatively easy to increase the transmission range of a base station by increasing its power, but that doesn't help users of mobile and portable radios, which are comparatively weaker, talk back to the base. Radio engineers work to balance the "talk-in" and "talk-out" of systems.

☐ Building Blocks – Duplex and Half-duplex Communications

When transmissions need to be relayed to include all users on a channel, a different class of radio station is used that can simultaneously receive a transmission from one user and retransmit it to all others. This capability is referred to as *duplex* communications. User radios typically can transmit or receive, but not do both simultaneously. As a whole, such systems of users and fixed stations are considered to be *half-duplex* because end users are transmitting or receiving, while stations relaying communications in the middle are doing both, simultaneously.

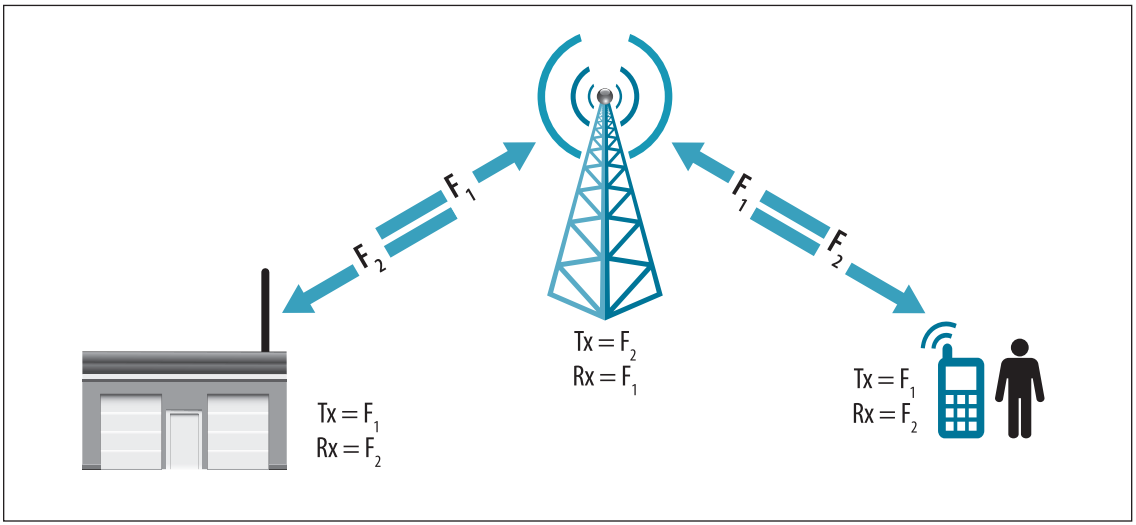
Telephones provide duplex communications. Few radio systems are designed to do so.

True duplex communications, as commonly experienced with telephones, allow the most natural forms of conversation. Since land mobile radio has evolved for one-to-many conversations in which at any moment there is one speaker and many more listeners, full duplex systems are unusual. As anyone who has ever been part of a telephone conference call can attest, having simultaneous "transmission" capabilities across all participants can actually impede communications at times.

☐ Building Blocks – Repeaters

Half-duplex relays are fundamental building blocks of public safety radio systems. "Mobile relay" is the official term for this class of station, but they're widely known as "repeaters." Repeaters as described have been used by public safety agencies for decades to automatically relay transmissions for system users who would otherwise be restricted in range by direct, simplex systems.

Figure 16-4: Half-duplex (Repeater) Radio Example



A repeater retransmits on one frequency what it receives on another, well separated from one another to reduce interference.

Repeaters are typically placed permanently with a well-situated antenna high up on a tower, building, or hilltop. From this vantage point, a repeater receives transmissions on one frequency and retransmits them on another. This serves to extend the effective range of a lesser powered radio, such as a portable, allowing other users of the channel to hear and talk with others at greater distances. Other fixed radio stations—at dispatch, for example—can also transmit through the repeater. These are known as *control stations*.

The repeater's frequencies have to be separated sufficiently from a spectrum point of view to keep the transmitter from overpowering the receiver. If not, the repeater's transmitter effectively prevents its receiver from "hearing" the relatively much weaker, distant signals. Some of the magic of radio engineering is dedicated to avoidance of these and more complex interference effects. Sophisticated antenna systems are used to isolate a repeater's transmissions from its receiver so it doesn't become the radio equivalent of an alligator: All mouth and no ears.

Figure 16-4 shows how frequencies are split between the repeater and its users. Note that the repeater's frequency pairing is the reverse of the other radios. Field users, including those at the station, transmit on Frequency 1 (F_1) but receive on Frequency 2 (F_2)—the repeater's transmission frequency. The repeater does the reverse.

☐ Building Blocks – Mobile and Portable Radios

Public safety agencies use mobile and portable radios to connect field operations with dispatch and other fixed stations, as well as among field users. Though lumped together by the FCC as "mobile" devices, vehicular and portable radios are considered by industry and the public safety community, itself, somewhat differently.

As might be imagined, portable radios are relatively handicapped compared to vehicular radios on two-way LMR networks due to limited transmission power and compromised antennas. They operate with much less transmit power than vehicular radios—about 5–10 percent of the latter's output power. Their antennas provide needed portability, often in exchange for efficiency, and are typically situated at something of an electromagnetic disadvantage compared to those on vehicle roofs. The human body, itself, tends to block radio waves that would otherwise be received or transmitted by the portable. To this, add the fact that portables can be and are often carried into locations far less friendly to radio emissions than the streets where vehicular radios operate.

Radio system design is hugely affected by whether primary coverage is sought for portable or mobile radio use. Two-way radio networks, voice and data alike, are built to take into account differences between fixed and mobile devices on the network.

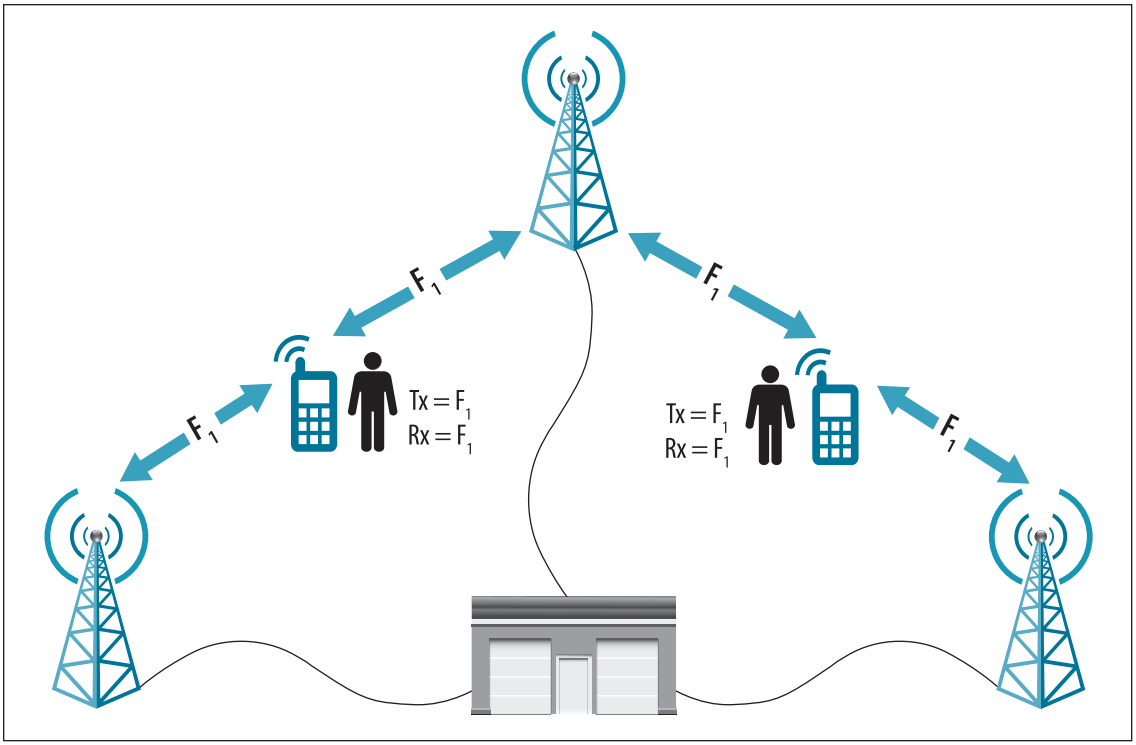
☐ System Building Blocks – Simulcast and Receiver Voting Systems

The technologies discussed so far have been in use for decades. In these *conventional* radio systems, there is a one-to-one correspondence between each frequency (or pair of frequencies in duplex or half-duplex operations) and a channel. In effect, channels are simply defined by who has and uses the designated frequencies within a given area of operation.

Coverage needs lead to use of simulcast systems where multiple sites transmit the same signal simultaneously to cover an area.

Large-scale, wide area systems have been built for years with conventional technologies. Public safety agencies have put up multiple repeaters to provide needed channel capacity for simultaneous operations and to cover wider areas. Capacity and coverage demands call for multiple repeaters at a single site in some cases and multiple sites in others. It's not uncommon to use multiple sites to provide coverage that can't be had from a single site. With such systems, users are relied upon to use the appropriate channel (i.e., frequency) depending on their job and location.

Figure 16-5: Simulcast Simplex Radio Example



It's possible with conventional systems to simultaneously transmit the same signal from multiple locations. This is referred to as *simulcasting*. It requires careful synchronization of the individual transmitters and a healthy backbone of microwave or some other form of dedicated telecommunications circuit to deliver the outbound signal to all sites simultaneously.

In the example shown in Figure 16-5, audio to be transmitted from all sites simultaneously originates from the central facility—a dispatch center, for example.

While simulcasting reduces the need for users to manually "steer" their radios by the channel selector knob as they move around a geographic area, it adds system complexity and a reliance on the circuits connecting to remotely operated base stations. It also brings a need for the system to deal with the common situation of two or more sites receiving a transmission from a field user. Just as a field user's radio will likely receive a transmission simultaneously from multiple sites, it will also likely be heard by multiple ones when it's transmitting.

Additional electronics are added to the heart of the system to select the best signal received by the sites. In the example shown in Figure 16-6, two sites might receive decent signals from a user, while the third site receives a weak signal. Central electronics pick out the best signal and pass it to users at the fixed facility.

This is known as a *simulcast* system with receiver voting. For practical purposes, the system can be thought of as a single base station with the wide, composite coverage provided by all the separate sites. The effect is a single channel that covers a wide expanse. While useful in low-traffic, routine operations, such wide-area, blanket coverage can be a problem during periods of high demand when the load across all sites can overwhelm a single channel.

The final conventional radio example to be presented here combines multiple technologies and adds a new one: Remote receivers. Actually, remote receivers have been depicted in the previous examples, too, but have been paired with their associated transmitters.

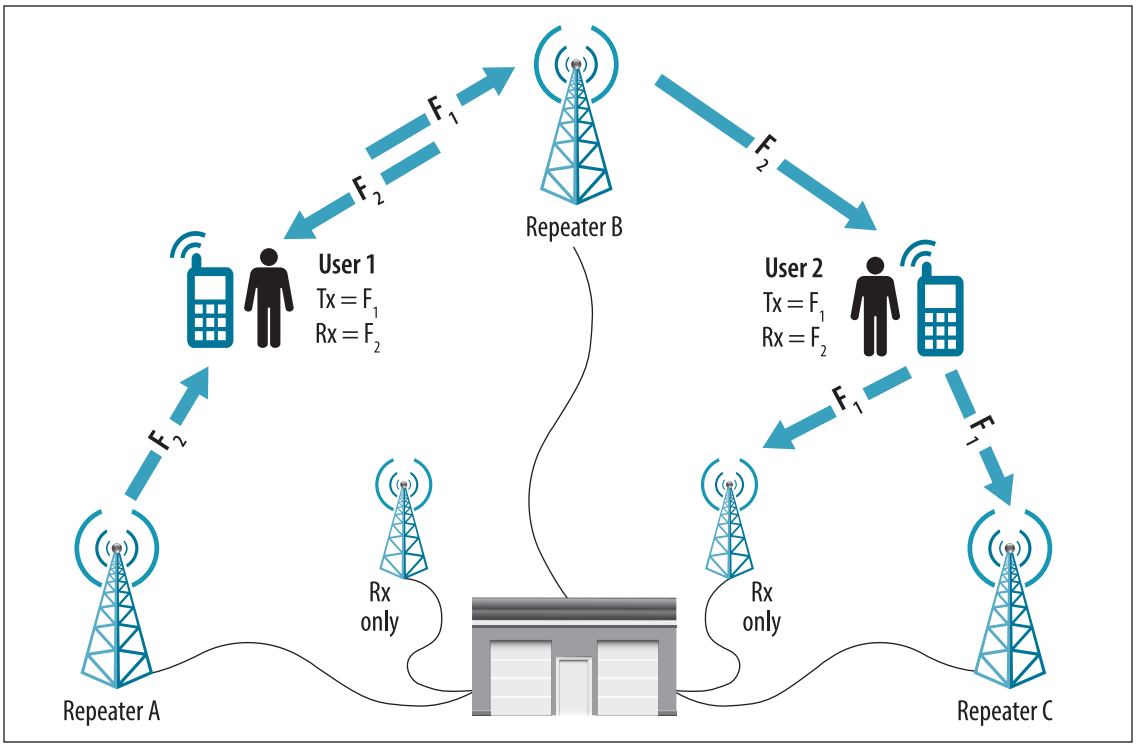
Remote receivers allow weaker signals to get into the system.

In Figure 16-6 on page 286, a repeater system is depicted with additional remote receivers. Sites labeled "Rx Only" are simply receivers that send back received signals to the central site where a *voter* can pick out the best received signal. Remote receivers are often used to accommodate portable radios that can "hear" the more powerful and well-situated fixed transmitter sites, but are unable to "talk" back to them due to the distance or terrain.

In this example, some possible receive and transmit paths have been omitted for the sake of clarity. It depicts a circumstance where Repeater A can be heard by User 1, but that user can only be heard by Repeater B. Repeater B can be heard by both users, but User 2 can only be heard by Repeater C and one of the remote receivers.

The combinations and permutations of which transmitter can be heard by which receiver—both fixed and mobile—are nearly endless in a large system. Imagine how complex this can become with dozens of fixed sites with multiple channels. It should be no wonder that radio engineers are needed to design and carefully tune all the components that make such an electromagnetic marvel operate!

Figure 16-6: Simulcast Repeaters with Remote Receivers



☐ System Building Blocks – Trunking

The next major technology used for public safety operations is *trunking*. Simply put, trunking is the means to share a limited number of frequencies between users, with each set of users having their own virtually private channels.

Trunking is widely used in telecommunications systems. Users of the public switched telephone network serving businesses, residences, and emergency response agencies worldwide are well experienced at using a trunked system—even if they are unaware of it. Complex technology assigns circuits (channels) dynamically upon requests for access, such as occurs when a telephone number is dialed. The newly assigned circuit may have just been used for an entirely different telephone call between different locations, but now is being reassigned.

Radio systems can be constructed to operate the same way. The primary value of trunking is channel efficiency. That is, rather than having sets of users occupy a channel fixed by frequency, leaving the channel empty at times and overloaded at others, the trunked system takes multiple channels and assigns them to sets of users as needed. This also provides groups of users that could never have a separate conventional channel to have a trunked one for private use.

The primary value of trunking is channel efficiency.

With a conventional system, three repeaters at a single site might have served police, fire, and EMS, individually, with all users from one of the disciplines operating on a single channel. With these three repeaters trunked, a nearly limitless number of virtual channels can be assigned and used without interference between users. However, the number of *simultaneous* conversations is still limited to the total number of talk repeaters at the site.

Trunking provides multiple virtual channels for separate conversations.

This brings up an important point: Most public safety trunking systems reserve one repeater at each site for the *system or control channel*. This is the channel of communications over which the radios talk among themselves behind the scenes to coordinate who goes to which frequency, at which site and what time, to become part of a conversation. This system traffic goes on nearly continuously as portable and mobile users move around between sites and change their channel selectors to become part of a different conversation.

While there is a direct correlation in conventional radio systems between channels and frequencies, trunked systems abstract the notion of a channel. Rather than being a fixed pair of frequencies, a trunked channel is a temporarily assigned repeater for use among a pre-defined group of users. In trunking parlance, the channel and its defined users are both known as a *talk group*.

A trunked channel is called a talk group.

Any individual user radio can be part of many talk groups. The user may, depending on agency policy and radio programming, choose to scan multiple talk groups during normal operations, just as they may have scanned multiple conventional channels with an earlier system. In a trunked system, the user radio literally notifies the system that it wants to be part of any conversations occurring among the selected talk groups. Still limited by the fact that the radio can only receive one transmission at a time, the user also has to select a single talk group on which to transmit using the radio's channel selector knob.

Trunked channels (talk groups) can be collapsed into one to bring otherwise separate users together.

Because trunked talk channels are set up and torn down as needed, end-user radios rely on the system to tell them when a talk group is becoming active and to get directions on where to tune. This takes place over the control channel, normally in a fraction of a second. As soon as an open repeater is available, which may actually be multiple repeaters if the network spans more than one site, the transmitting radio is allowed to talk and all other radios in the talk group automatically tune to the transmission frequency(s).

All talk group conversations go through the system. A central controller connected to all sites and each repeater steers system resources to maximize capacity according to preset parameters. The system can be programmed, for example, to give certain user groups preference over others as they queue up waiting for assignment of a channel. It can automatically spread conversations over multiple overlapping sites to reduce bottlenecks.

Trunked System Policies

The complexity and configurability of trunked systems **require** great care in implementation and ongoing management. Design such complex systems through careful needs analysis (Chapter 6), implement them using functional acceptance tests mapped to user requirements (Chapter 10), and manage their flexibility through strict adherence to both technical and operational policies and procedures (Chapter 12).

Trunked systems can also be managed on the fly by dispatchers and system administrators to collapse multiple talk groups into a single one. This has a strong implication for interoperability. Where several talk groups may be operating independently from one another during an incident, and thus unable to communicate between their various users, a dispatcher appropriately authorized can combine the talk groups into one. All users of the affected talk groups can effectively be moved to a common one. While increasing interoperability, this also has the effect of increasing traffic on the newly combined channel.

☐ Trunked System Pros

Trunked systems are commonly built with all the simulcast and remote receiver capabilities described for conventional systems. In addition, the system-wide ability to create virtual channels and assign radio resources as needed brings great flexibility to user agencies. The system, itself, can contribute by balancing demand across physical radio resources. Again, the greater channel efficiency of trunked systems may mean they are the only choice in jurisdictions where spectrum resources have otherwise been exhausted.

☐ Trunked System Cons

With all of this power, there are downsides to trunked radio systems. First, they are costly. Agencies can expect to pay upwards of 50 percent more for the cost of a trunked system over a conventional one with the same number of sites and radios.

Second, all this power comes at the cost of greater complexity and potential for failure. While modern system design calls for "fail-soft" systems that still operate in a degraded mode as components fail or become unavailable, trunking still ultimately depends on fixed infrastructure to work. The final fail-soft mode for trunked radio systems is to operate conventionally—that is, with radios talking directly on pre-designated frequencies chosen for specific purposes.

Communications in Buildings and Tunnels

Emergency responders face great coverage challenges in urban areas, as well as rural ones. Where the challenge in mountainous terrain is overcoming natural obstacles, radio systems in more populous areas are equally challenged to overcome manmade mountains, canyons, and caves. Since the earliest days of radio, engineers have looked for ways to provide communications in buildings and tunnels.

Radio system coverage in buildings and tunnels requires additional infrastructure.

Fixed, point-to-point communications in such environments are relatively straightforward. On the other hand, communications with field units—whether vehicular-mounted mobile radios or personally-carried portables—is the biggest challenge. Portable radio communications are most difficult to accommodate, of course, because of their relatively low output power and limited antennas. Portable communications are further handicapped by how they are generally used, being worn in close proximity to the body, which serves a lot better as a signal absorber than reflector. Recognize that portable and mobile uses are similarly affected by coverage challenges, only to different degrees.

SAFECOM Library: Trunked System Resources

Several useful reports on trunked radio are on the SAFECOM website, including:

Comparisons of Conventional and Trunked Systems (1999):
www.safecomprogram.gov/library/Lists/Library/DispForm.aspx?ID=239

Operational Best Practices for Managing Trunked Land Mobile Radio Systems (2003):
www.safecomprogram.gov/library/Lists/Library/DispForm.aspx?ID=219

How 2 Guide for Establishing and Managing Talk Groups: www.safecomprogram.gov/library/Lists/Library/Attachments/216/How_to_Establish_and_Manage_Talk_Groups.pdf

☐ Area Solutions

The most basic technique used to improve communications in buildings and tunnels is to put additional system sites in denser urban areas. This increases the fixed station (base or repeater) signal into nearby buildings and provides it a somewhat stronger signal from the field unit. Because the greatest weakness is usually the fixed station's ability to "hear" the portable transmission, a more advanced technique is not to add entire fixed stations (transmitters and receivers), but more receivers strategically placed. This allows the relatively weak portable signal to "get into the system" from more places.

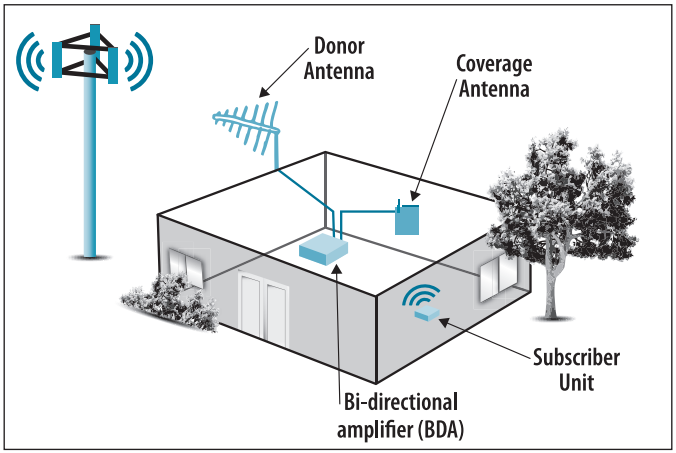
While basic, this approach can be satisfactory in some locales and reduce requirements for specialized technology and the additional expense of in-building systems. System managers face an ongoing challenge in assuring that new construction in and around the areas of interest doesn't reduce coverage or otherwise interfere with the balance achieved.

☐ Point Solutions

More and more often, peripheral technology is being used. This requires placement of special repeating equipment within buildings, tunnels, and other signal-challenged areas.

Bi-directional Amplifiers (BDAs) are placed within the building to, as the name implies, improve signals both inbound and outbound. Internal and external antennas are linked by the BDA to capture weaker signals from within and retransmit them beyond, and vice versa. Large structures may require a more elaborate, distributed system of internal coverage antennas connected together, then linked to the outside world through a single "donor" antenna.

Figure 16-7: Bi-directional Amplifier Example



Source: PSWN. Novembet 2002

Some areas, such as tunnels, are well suited to use of a special type of distributed antenna system built from radiating coaxial cable. Traditionally, coaxial cable (coax) of various forms is used to connect radios to their antennas. Properly speaking, the cable is part of the antenna system, but is intended to quietly move signals from each end to the other.

Radiating cable, on the other hand, is constructed to "leak" signals in and out along its length. This can be a very effective sort of distributed antenna, although, as might be expected, some careful engineering is needed for systems of this sort. Figure 16-7 shows an example of a BDA.

☐ Governmental Regulation of In-building Coverage

There has been increasing interest post-9/11 in local ordinances requiring building and structure owners to assure public safety radio coverage inside. While the need for coverage improvements is indisputable, systems are sufficiently specialized that they don't promise to improve communications interoperability outside of the improved coverage of a single, targeted system. In other words, they don't broadly improve interoperability.

A 2002 report by PSWN on the topic concluded that such ordinances "have no noticeable impact on interoperability between public safety organizations."[101]

101. *Public Safety In-Building/In-Tunnel Ordinances and Their Benefits to Interoperability Report*, Public Safety Wireless Network Program, November 2002, p. 14.
See www.safecomprogram.gov/library/Lists/Library/Attachments/293/Public_Safety_In-Building_In-Tunnel_Ordinances.pdf.

Figure 16-8: Plaquemines Parish (Louisiana) Radio Tower – August 29, 2005

Source: Plaquemines Parish website, **www.plaqueminesparish.com**.

Satellite Communications

Natural disasters have brought increased interest in satellite communications to overcome the damaged and destroyed land-based radio systems. Hurricane Katrina, which ravaged the United States Gulf Coast late in August 2005, widely disrupted radio systems. Not only was cellular telephone infrastructure damaged and nonexistent in many places, but public safety radio systems were disabled in many locations (see Figure 16-8). Whenever basic agency radio systems are damaged, interagency communications suffer.

Satellites provide a backup means of communicating, particularly when terrestrial infrastructure is nonexistent. They are regularly used in wildland fire and other disasters, both to provide telephone services and data communications. In a traditional or newly created wilderness, satellite communications may be the only way to talk out from an incident scene.

Satellite services are available from a variety of vendors. Some are provided by way of *geosynchronous* satellites that appear to the user to be fixed at a spot in the sky. At an altitude of 22,241 miles, such satellites orbit at the same rate the earth rotates. Similar to direct broadcast satellite (DBS) television, these services require a fixed antenna that is pointed at the satellite or one that is electronically steered to keep itself so.

Other services are provided through low earth orbit (LEO) or medium earth orbit (MEO) satellites that are relatively much closer, though still far distant compared to cellular and terrestrial public safety radio infrastructure. LEO satellites orbit in a band from a few to several hundred miles above the earth. This distance still challenges the portable communications needs of first responders.

Despite their value for disaster telephone and data services, satellites are not a complete replacement for terrestrial voice radio systems used by public safety for several reasons:

- **One-to-many communications are inadequate.** Voice communications as most commonly used via space is limited to telephone-like services where a user can dial up another telephone user—whether on the public switched telephone network or elsewhere on a satellite system. Satellites do not offer the *immediate*, one-to-many sort of radio conversations needed by public safety responders.
- **Coverage is inadequate.** First responders moving about with portable radios need coverage in all areas. Less penetrating than even cellular telephone signals, satellite signals don't reach far inside buildings or into dense vegetation. Public safety radio systems are engineered to provide coverage far beyond what satellite systems provide.
- **Portable capabilities are inadequate.** Even LEO satellites are many times further away in distance than traditional land mobile radio infrastructure. Since both use radio frequencies to communicate, satellite signals are reduced in strength even more across the distance, requiring bulkier antennas and higher power. Even with adaptive power modes that reduce battery demand, satellite handsets require more battery power than a responder's standard portable radio transmitting a much shorter distance. The demanding emergency response environment leads to greater power consumption as users move in and out of clear view of the sky.
- **Capacity is inadequate.** Communications between emergency responders on-scene during events is frequent. Many channels are needed for larger events, such as those that would take out terrestrial infrastructure, and near-instantaneous communications is needed in most cases. A single responder often needs to communicate instantly with dozens of others. Satellites don't provide this ad hoc broadcast capability.

Satellite communications are vital in response to disaster. Their primary value is as a replacement for cellular and other terrestrial telephone systems. In times of disaster, there may be no alternative. Running a close second in value, data communications via satellite are indispensable from any location out of range of terrestrial wireless systems due to distance or events.

VoIP in Voice Systems

Voice over Internet Protocol or VoIP for communications has arrived. Most simply, it is the semi-standardized means of taking voice or other audio that has been digitized, then pushing it over networks similar to any other form of data. Internet Protocol (IP) is part of the suite of standards that powers—imagine this—the Internet and most other data networks today.

We refer to VoIP as "semi-standardized" because there are limitless ways to move digitized voice over IP-based data networks. It's not as simple as just throwing voice data packets on the wire and reassembling them at the end. The process is much more complex and requires more communications between sending and receiving systems than just the voice data. Different means are used by different vendors and for different purposes to control the "envelope" of what we would consider a conversation that is stuffed with voice bits and bytes.

☐ Basics of Digital Audio

Digitized audio has been passed over backbone telecommunications circuits for years. VoIP differs in that the audio (voice or otherwise) is passed over modern data networks that can route and reroute packets across a variety of intermediate networks. They can, and do, pass over networks used for other data purposes. There are tradeoffs though.

Voice communications is much more time-sensitive than data communications. Network delays that would be unnoticed by the typical data user become noticeable and even intolerable when the user is trying to carry on a two-way conversation. Most cellular and many other telephone systems exhibit such delays and we all are familiar with how it affects normal conversation.

This isn't an effect of VoIP, per se, but rather of digital networks being slowed due to demand or disruptions. IP-based networks traditionally used for data will dynamically adapt to such factors and are designed to trade speed for certainty of delivery. That is, the network will try and try again to get a packet that has been lost or damaged so it can package them all up reliably and deliver the complete lot at once.

Voice communications, on the other hand, can survive an occasional dropped packet better than it can handle delays. Each packet contains a small piece of audio information. The human brain is remarkably able to extract an intelligible message from disrupted audio.

☐ VoIP in Public Safety Communications

Public use of VoIP telephone systems has brought all sorts of challenges to the public safety world, particularly in delivery of 9-1-1 services. However, it has proven to be a boon in other ways.

Transmission of voice and other audio over IP-based data networks has rapidly become a critical, underlying means of connecting agencies for interoperability. VoIP is used to interconnect private telephone systems, dispatcher consoles, and parts of the radio infrastructure. For practical purposes, it is an underlying protocol rather than an end-user application, though.

For example, dispatch consoles have been connected for decades to remote base stations through dedicated telephone circuits—typically analog ones much like plain old telephone service (POTS—seriously). As telecommunications infrastructure has moved to digital from analog, lines that tie one fixed point with another have also migrated. VoIP is increasingly used in this case to move the dispatcher's voice to the radio transmitter and the user's voice back from the receiver.

☐ A Fundamental Tool

VoIP has rapidly become a fundamental tool connecting pieces of public safety communications systems. While it may be an underlying protocol for connecting systems at an audio level, it doesn't solve the problems posed by any gateway between disparate radio systems, as described further in the next section, **Approaches to Interoperability**.

VoIP is a fundamental tool, but not a silver bullet.

VoIP is the current, logical choice for connecting pieces of a system where dedicated telephone circuits may have been used in the past. As any higher level communications protocol, it relies on underlying network infrastructure to carry data. VoIP offers the possibility of passing voice over networks used for other data communications, but in the process naturally puts those packets in contention with other traffic on the network.

Critical systems need dedicated network services.

The state of the art in VoIP telephone systems is to use dedicated data networks—physical or virtual—to reduce that contention and assure acceptable service. Critical public safety systems need high-quality service, as well.[102]

☐ "Radio over IP"

The term "radio over IP" has been used to describe VoIP used in radio applications. It's a confusing term and one we advise against using. It's the logical equivalent of "Air over Esperanto."

Without getting deep into theory,[103] data being transmitted using Internet Protocol can pass over many different physical mediums, both wired and wireless. Voice, as an application, runs over IP and other protocols, then over one or more mediums en route to one or more final destinations. "Radio over IP" is backwards.

In addition, modern radio systems use VoIP to move voice and other audio, such as signaling tones, across their infrastructure. They don't, however, use it over the airwaves. Land mobile radio systems reassemble the voice packets and transmit them over the air using the system's fundamental operating mode—whether analog or digital, as in P25. This is analogous to what a receiver does with digital music before it sends it to its speakers in a classic stereo system.

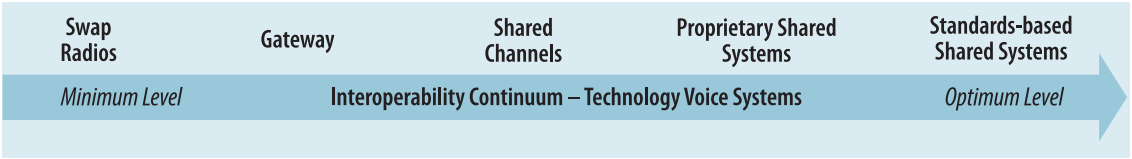
VoIP is a fundamental tool in today's telecommunications systems, but it's not a silver bullet.

Let's move on to how these technologies are used in pursuit of interoperability.

102. A decade ago, the Public Safety Wireless Network Program released an assessment of VoIP for public safety radio systems. See *Software-Enabled Wireless Interoperability Assessment Report – Voice-Over-Internet Protocol Technology,* December 2001. See www.safecomprogram.gov/library/Lists/Library/Attachments/300/VoIP_Technology_Assessment.pdf.

103. The Open Systems Interconnection (OSI) model is fundamental in telecommunications theory, having originated in 1977. It describes systems in terms of a layered stack and defines interoperability between layers. Radio is a low, physical layer, while Internet Protocol is in the middle. Voice as an application of a system would be at the top of the model. For further information, see http://en.wikipedia.org/wiki/Open_Systems_Interconnection.

Figure 16-9: Continuum of Interagency Voice Communication Technologies



Source: Adapted from *Interoperability Continuum*. © U.S. Department of Homeland Security.

Approaches to Interoperability

Communications interoperability has been hindered due to the simple lack of a common vocabulary for discussing the topic. SAFECOM's *Interoperability Continuum* has improved the situation greatly through practitioners' definition of five critical dimensions of interoperability. It also provides simple measures for assessing relative stages of development. Of the five dimensions, technology in particular is the subject of only one. Proportionally, this continuum effectively represents the fact that the great majority of work in achieving interoperability is in the *human* aspects of governance, procedures, training, and familiarity through frequent use.[104]

The *Interoperability Continuum* provides a simple, effective description of the technology choices available to provide interagency voice communications. These means of communications provide a convenient way of examining the range of choices, sophistication, and completeness of voice radio technology. As in the *Interoperability Continuum*, technology choices are shown in Figure 16-9 and listed below in order of increasing capabilities.

Let's take a look at these approaches individually.

Technology Approach: Swap Radios

As noted in the SAFECOM description, agencies have swapped radios to enable communications among themselves since the earliest days of public safety radio usage. To this day, agencies exchange spare radios with key partners on incident scenes for the sake of interoperability. In some cases, they do so even though their respective systems are otherwise technologically compatible. For example, this may occur because the users either don't have common channels programmed into their radios or they use different channel naming and naming conventions. Whether due to technological incompatibilities or a lack of prior planning, the end result is the same: a conclusion that this, the most basic means of interoperability, is necessary.

Swapping radios or maintaining a cache of standby radios is an age-old solution that provides results but is often time-consuming, management-intensive, expensive, and may only provide limited results due to channel availability.

— *SAFECOM Interoperability Continuum*

104. SAFECOM's *Interoperability Continuum* is included in this Guide as Appendix G.

During incidents when agencies respond with incompatible equipment—using different frequency bands, for example—swapping radios provides responders the ability to talk to the other agency via that other agency's system. Obviously, while this can and does work for very simple operations, it becomes unworkable as more and more agencies arrive.

A common use of this technique is in deployment of radio caches. A radio cache is simply a supply of radios, typically portables, held aside for larger incidents. The cache may include spare batteries, antennas, and carrying cases to simplify deployment. Typically, the cache is left stored away until a request is made for its deployment.

The use of radio caches is, unfortunately, fraught with pitfalls. Common troubles include:

- Unknown or nonexistent procedures for request and deployment
- Inadequate maintenance of the equipment, particularly batteries that can be damaged from both too little and too much charging
- Poorly documented channel programming, leading to inadequate usage
- Lack of training on the equipment, its available channels, and their appropriate use

By far the majority of multiagency emergencies handled day-to-day in this country arise and are handled much too rapidly for caches of radios to be deployed. On the other hand, large-scale emergencies often call for the use of cached radios to allow multiple responding agencies use of a single system.

Two examples of cached radio equipment are notable in this approach to communications interoperability.

☐ National Interagency Incident Communications Division

During the seemingly annual natural disasters that plague the American West, the National Interagency Fire Center (NIFC) in Boise, Idaho, provides logistical support to federal, state, tribal, and local agencies. A prime resource is radio equipment from its communications cache.

NIFC's National Interagency Incident Communications Division (NIICD),[105] operated jointly by agencies of the U.S. Departments of Agriculture and the Interior, provides equipment in response to natural and manmade disasters of all sorts. Its cache was heavily tapped for equipment and trained ICS Communications Unit personnel in response to the Gulf Coast following Hurricanes Katrina and Rita.

The NIICD radio cache is jointly maintained by the U.S. Departments of Agriculture and the Interior.

NIICD cache equipment is used for standalone communications networks where needed to support large-scale emergency response, typically involving many agencies.

☐ Beltway Sniper Incidents

During a 3-week period in October 2002, two men terrorized the Washington, D.C., area through seemingly random sniping incidents that left 10 people dead. Each of the incidents brought local first responder agencies together, but more broadly, law enforcement agencies from across the region and all levels of government convened in pursuit of the attackers.

Montgomery County (Maryland) had a supply of new, unused radios that was pressed into interagency service.

Montgomery County, Maryland, was the location of the earliest and majority of the attacks. By coincidence, the county happened to be in the middle of deploying a new radio system for its public safety agencies. System infrastructure was largely in place and end-user equipment was warehoused for pending installation.

When joint task force operations involving many law enforcement agencies ensued, the new radio system was activated and the new radios distributed to provide interagency communications. In effect, cached equipment was used to provide a common communications environment, much as is done in the West during remote wildfires. Outside agencies used their own communications capabilities as well as they could considering varying coverage limitations, but the distribution of Montgomery County radios to cooperating responders and investigators provided simple, but much needed communications interoperability.

105. For more information on the NIICD, see www.nifc.gov/NIICD/index.html/.

Technology Approach: Gateways

Gateways (or audio bridges) retransmit across multiple frequency bands, providing an interim interoperability solution as agencies move toward shared systems. However, gateways are inefficient in that they require twice as much spectrum because each participating agency must use at least one channel in each band per common talk path and they are tailored for communications within the geographic coverage area common to all participating systems.

—*SAFECOM Interoperability Continuum*

Response to the Beltway sniper incidents involved another approach to interoperability: Connecting different systems or channels through a gateway. In order to provide communications between users of its old and new systems during the unanticipated activation, Montgomery County linked channels together across the two. The effect was to provide a common channel shared across each.

The term "gateway" is used for any of a number of means of patching transmitted and received audio from one source to another. Technically, it is a bit more complex, requiring controlling circuitry to initiate transmission on one side of the equation when something is received on the other. Whether involving radio channels, telephone calls, or another source of audio, channel patching is another age-old approach to connecting users from one system to those on another.

In its earliest form and still practiced today, a dispatcher at a communications console can patch the audio from one channel to another despite the fact that there might be huge technological differences between the individual systems. This is the same approach, technically speaking, that a dispatcher would use to patch a telephone call to a radio channel and vice versa. The effect is that the two communications channels are collapsed into one using bridges or gateways between different telecommunications systems.

Modern technology has made it possible to do this not only in increasingly complex ways from the dispatch console, but also via remotely operated gateways. The simplest gateway devices are no larger than a pack of cigarettes, limited in size physically more by the space needed for connecting cables than by the complexity of their internal electronics. This sort of portability allows for devices that can be fielded to patch together first responder channels. Though most commonly used to bridge radio channels in different frequency bands, many of the devices can also be used to link "push to talk" radios[106] to other two-way audio sources, such as landline, cellular, and satellite telephones.

106. "Push to talk" radios are the standard type of radios used by public safety agencies. Whether portable, mobile, or installed at a fixed location, they're distinguished from other forms of radios by the fact that some sort of switch is manually or electronically actuated to initiate transmissions from the radio. The term "push to talk" has been used to distinguish the familiar two-way radio from other types of portable communications devices, such as cellular telephones.

Increasingly sophisticated networking technology allows gateways to be connected between dispatch consoles and other audio sources across data networks. Audio is digitized, addressed, and routed across networks just like any other form of data.

Gateways patch transmitted and received audio from one source to another.

As mentioned previously, Voice over Internet Protocol (VoIP) can be used for moving audio across data networks between radio systems. Those networks can even connect a gateway on one radio system to another that is geographically distant, providing radio end-users at either location a means to talk to each other. This isn't 21st century James Bond wizardry, though. Amateur radio operators have been using the technology since the late 1990s and now have a worldwide network of more than a thousand Internet-connected radio nodes serving every continent, including Antarctica.

VoIP is being used to connect systems across data networks using gateways.

Whether as simple as a dispatcher's console patch or as complex as a worldwide VoIP network, gateways are widely used to connect distant and disparate channels of communications. While commonly used, this approach to interoperability has serious limitations and brings challenges of its own.

☐ Gateway Issue: Capacity

By design, gateway devices linking together multiple channels of communications—radio or otherwise—end up repeating traffic from one channel to others. This reduces the original load-bearing capacity of each.

When two actively used channels are linked, the amount of traffic on each will increase significantly. Popular gateway devices allow many more than two channels to be linked, potentially multiplying the amount of traffic on each by the number of connected channels.

Obviously, any moderately used channel can be heavily taxed by patching together other, similarly used channels. This can result in serious contention for access to the channels, not to mention an increased level of traffic that may not be relevant to the original channel users.

Separate channels of communications are necessary during emergency response in order to segment responsibilities and account for the limited capacity of any individual channel. Indiscriminately used, gateway devices can disable the channels they interconnect by overwhelming them, literally or practically, with too much traffic.

TMI: How much do you want to communicate?

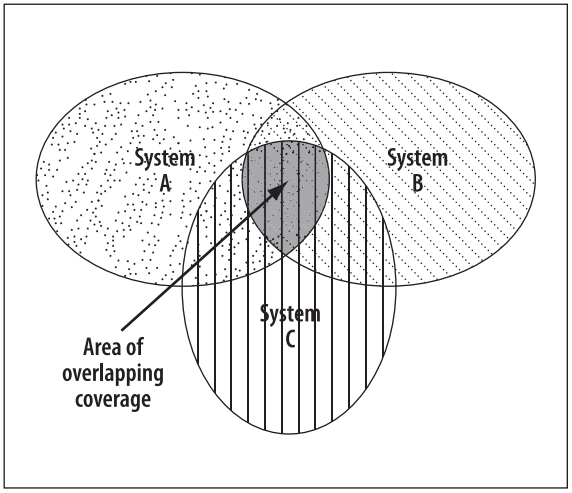
In the wide world of communications, the term "signal-to-noise ratio" is used in talking about the eventual *intelligibility* of exchanges. The principle is that a signal has to be significantly stronger than any background noise for effective communications to occur. Anyone who has ever observed the volume level of conversation rise at a party as attendees increasingly struggle to be heard over one another has witnessed how the signal (conversation) can be lost amid background noise.

Back in the field, first responders often struggle to catch transmissions relevant to their jobs during incidents as radio transmissions multiply many times over. The challenge of too much information, of the signal being lost among "noise," is equally as disabling as not getting enough information.

☐ Gateway Issue: Coverage

It might not be intuitively obvious, but gateways can only link first responders at an incident scene in areas of overlapping coverage between the linked systems. In other words, once outside the range of one's home system, the system user doesn't benefit by the gateway. The gateway doesn't extend the geographic range of the individual systems that are interconnected.

Figure 16-10: Overlapping Coverage of Systems



Conversely, and somewhat perversely, linked systems can lead to too much, yet inadequate, coverage. For example, linking together Systems A, B, and C, as depicted in Figure 16-10, means that users of System C will be heard across the range of all systems, but still can't talk to any other system user when traveling outside of the range of their own. This can and does lead to systems interfering with others beyond their normal coverage areas. More critically, it also leads to communications failures in areas where responders were previously heard, but can't talk from once they get there.

Radio coverage is a complex issue under the best of circumstances. It becomes even more so when multiple systems are linked together. Coverage becomes *asymmetrical*. That is, radio users can be heard in places where they can't talk from. Again referring to Figure 16-11, System A users can talk to users of both Systems B and C—as long as they are within the coverage footprint of System A. Once outside of it, they can't speak to anyone through the gateway *even though they are in the range of the other, linked systems*.

Gateways can easily lead to *asymmetrical* radio coverage.

☐ Gateway Issue: Transmitter Licensing

If the above technical complexities of gateways aren't daunting enough, their legal operation poses additional challenges. Unfortunately, a proliferation of gateway devices in recent years has led to some being used in operations outside the authority granted by the FCC for the respective interconnected systems. This is a rather obtuse and occasionally confusing subject, but we'll try our best to explain it here and provide reference to other sources.

Basically, FCC licenses are required for practically all radio transmitters used in public safety communications systems. Each portable, mobile, and fixed station radio is covered under a license that specifies, among other things, an **area of operation**—the area in which the radio can transmit. Most classes of fixed stations, such as base stations and repeaters, are licensed for a particular physical location, height above ground, and maximum power. Typically, end-user radios are licensed for operations only across the agency's jurisdiction or within a given distance from a fixed point.

Most transmitters are licensed for a limited area of operations.

Mutual aid and other types of interagency operations are often conducted outside of one or another agency's jurisdiction—by definition. While the visiting agency's radio system may provide incidental coverage outside its jurisdiction, it is illegal for end users to use any system outside of its licensed area of operation. This is done to protect other legitimate use of the licensed radio frequencies and to allow reuse of spectrum elsewhere.

When gateways are used to interconnect systems, the potential arises for radios to be operated outside their licensed area of operation. In addition, a portable or mobile radio connected to a gateway becomes a different class of radio station. In essence, it's no longer legally an end-user radio, but rather a type of fixed station. While the FCC can grant "Special Temporary Authority"[107] under emergency circumstances to operate an unlicensed transmitter, nothing beats preplanning and licensing.

Rely on FCC-certified frequency coordinators for guidance on gateway licensing.

107. The FCC maintains a web page describing the procedure for obtaining Special Temporary Authority for a station. See http://transition.fcc.gov/pshs/services/sta.html.

FCC Rules and Regulations governing public safety radio systems (Part 90 – Private Land Mobile Radio Services) provide latitude for alternate use of licensed radio stations during emergencies that have disrupted communications facilities.

FCC Rules and Regulations
47 C.F.R. §90.407 Emergency Communications

The licensee of any station authorized under this part may, during a period of emergency in which the normal communication facilities are disrupted as a result of hurricane, flood, earthquake, or similar disaster, utilize such station for emergency communications in a manner other than that specified in the station authorization or in the rules and regulations governing the operation of such stations. The Commission may at any time order the discontinuance of such special use of the authorized facilities.

The FCC-certified public safety frequency coordinators[108] are the best source of guidance in navigating the complexities of licensing transmitters used to interconnect radio systems through gateways.

☐ Gateway Issue: The "Ping Pong" Effect and Other Complexities

Despite the relative simplicity with which gateways can be deployed to connect responders, they can negatively impact the systems they interconnect. The National Institute of Justice (NIJ) CommTech Program[109] has worked for several years testing gateway devices and sharing lessons they have learned. Much of what we know about their use in the public safety environment comes from NIJ testing.

One technical complexity that has been described is referred to as the "ping pong" effect. It occurs when a gateway is used to connect users through two or more repeaters—fixed radio stations that receive transmissions from portable, mobile, or other fixed stations and repeat them for other radio users to hear more widely and clearly. Without careful tuning, gateways connecting repeaters can endlessly cause the other to transmit.

Similarly, multiple gateways on the scene of an incident or inappropriately configured ones can actually *dis*-able, rather than enable interagency communications. This can happen when uncoordinated use of multiple gateways leads to systems talking in an endless loop.

108. For more information on FCC-certified frequency coordinators, see http://transition.fcc.gov/pshs/public-safety-spectrum/coord.html.

109. CommTech was previously the Advanced Generation of Interoperability for Law Enforcement (AGILE) Program. Further information about the program can be found on its website. See www.nij.gov/nij/topics/technology/communication/welcome.htm.

Dueling Radios

"By far the most challenging technical aspect of the deployment of the [gateway] was in interfacing with the repeater systems of the participating agencies. In systems in which a radio interfaced to the [gateway] is transmitting to a receiver site through a repeater, due to the length of the squelch tail, a repeater could stay up long enough to bring the radio connected to the [gateway] back up before the repeater goes down. Then because the radio is back up, the repeater could come back up, bringing the radio back up; and so on. This effect is referred to as the 'ping pong' effect."

Advanced Generation of Interoperability for Law Enforcement (AGILE)
Report No. TE-00-04, 23 July 2001
www.safecomprogram.gov/library/Lists/Library/Attachments/257/Operational_Test_Bed.pdf

Despite the issues described here, gateways play an important part in many interagency communications systems today. They offer the portability and flexibility necessary to link various radio systems, frequency bands, and protocols existing across public safety agencies. Well used, they provide an important technological approach to interoperability.

Technology Approach: Shared Channels

Historically, the most common means of interagency communications by radio has been through the use of shared or common channels. As noted in the *Interoperability Continuum* excerpt, users of the same frequency band have the added option to share channels for interoperability. These channels may be for direct or unit-to-unit conversations within a limited range on-scene or through repeaters programmed into their respective radios for greater range.

Although fragmented radio spectrum use reduces the potential, shared channels provide a low-cost and effective means of interagency communications in locales where users have the benefit of a common frequency band between their agencies. Commonly shared or formally designated interoperability channels now exist across all major public safety bands. In some jurisdictions, gateways are used to link designated shared channels between different bands, combining the use of multiple approaches to interoperability at the cost of duplicating transmissions across multiple channels.

Interoperability is promoted when agencies share a common frequency band and are able to agree on common channels. However, the general frequency congestion that exists across the United States typically places severe restrictions on the number of independent interoperability talk paths that are possible.
— *SAFECOM*
Interoperability Continuum

Palmetto 800 System Gateway Guidelines

The state of South Carolina maintains guidelines for using gateways to interconnect other systems and users to the Palmetto 800 System. The purpose, objectives, and benefits of the guidelines are clearly stated:

Purpose: To maintain the availability and functionally of the Palmetto 800 System for the primary system users.

Objectives:

a) Ensure the integrity of the Palmetto 800 System

b) Provide interoperability options

c) Manage system loading

d) Establish a guideline for the use of interconnects

Benefits:

a) Improve safety

b) Reduce interference and interconnect technical problems

c) Provide alternate 800 MHz service for special events and emergencies

For more information, see http://cio.sc.gov/councilscommittees/palmetto800/.

FCC Designation of Shared Channels

In addition to any specific frequency (or pair of frequencies for a repeater) adopted by convention by agencies for shared use, FCC Rules and Regulations designate specific frequencies for interagency communications. The number and availability of these frequencies vary considerably by band, as well as location.

Putting Shared Channels to Work

Use your radio technical resources and frequency coordinators to learn if there are FCC-designated shared channels available for use. There may be existing shared channel plans that you can take advantage of, but know the limitations and licensing requirements before putting them to use.

Five VHF-high band (150-174 MHz) frequencies, ten UHF (450-470 MHz) frequency pairs, and five 800 MHz frequency pairs have been designated for more than a decade for interagency use. However, the VHF and UHF frequencies have been incorporated into interagency communications plans differently across the country, and often not at all. In many cases, the frequencies have been assigned for specific agency use. The 800 MHz pairs were designated solely for interagency use and provide key shared channels capability where this band[110] is well used.

110. The FCC created the National Public Safety Planning Advisory Committee (NPSPAC) in the 1980s to guide rules for a segment of the 800 MHz band dedicated to public safety use. This spectrum is commonly referred to as the "NPSPAC band" or "800 MHz NPSPAC."

FCC narrowbanding rules and regulations split out additional channels from the traditional, 25 kHz ones, though they won't be wholly available until operations on adjacent channels migrate to narrowband. In 2000, the FCC designated five additional VHF frequencies and four UHF frequency pairs for interoperability use. These are narrowband (12.5 kHz) channels. Since January 1, 2005 their use under FCC rules for interagency communications has taken precedence over other licensed uses.

Many more channels specifically designated for interagency use are available in the 700 MHz band for regions of the country where this spectrum is clear of television broadcasters. As public safety systems are built in this frequency band, agencies will have access to more than 100 shared channels whose use is governed by state-level decision making bodies.[111]

Technology Approach: Shared Systems

The growing complexity and cost of radio systems have combined with serious needs for improved interoperability to push public safety agencies toward sharing of systems. Whether built of proprietary technology or based on accepted standards, shared radio systems offer economies of scale, less redundancy, and inherent interoperability of the chosen technologies. While sharing a radio system doesn't alone provide agencies with communications interoperability, it does provide core parts of the technical foundation.

Radio systems have been shared as long as public safety has been using the technology. In relatively recent history, however, technical innovation has followed their need to manage rising costs, crowded radio spectrum, and difficulties communicating with other agencies migrating to other frequency bands and technology. System sharing has come as a natural solution to each of these needs.

Regional shared systems are the optimal solution to interoperability. While proprietary systems limit the user's choice of product and manufacturer, standards-based shared systems promote competitive procurement and a wide selection of products to meet specific user needs. With proper planning of the talk group architecture, interoperability is provided as a byproduct of system design, creating an optimal technology solution.

— *SAFECOM*
Interoperability Continuum

111. The FCC maintains a web page explaining use of 700 MHz interoperability spectrum in greater detail. See http://transition.fcc.gov/pshs/public-safety-spectrum/700-MHz/.

☐ Proprietary Shared Systems

Trunking, as previously discussed, has been adopted as the primary means of sharing limited radio channels while still providing individual users privacy and autonomy. The earliest trunked radio systems were built of proprietary technology, limiting choice of system components and generally increasing costs through reduced competition and vendor lock-in. Many such systems are still in use today, both in single agency and shared use.

Shared systems offer economies of scale, less redundancy, and inherent technological compatibility.

Proprietary or not, shared systems provide the technological compatibility necessary for interoperability between their users.

☐ Standards-based Shared Systems

The simplest shared system is where one or more channels is used conventionally (i.e., not trunked), either analog or P25 digital, between agencies. There is no proprietary aspect of such an approach and radios from various manufacturers can be mixed and matched to create the system. While channel efficiency of conventional systems can't approach that of trunked ones, they are a cost-effective option and provide opportunities for sharing of system infrastructure and backbone networks. Individual channels can be dedicated by agency with others shared for interagency communications.

P25 is the public safety standard for digital radio.

Because channel demand has overwhelmed available public safety spectrum, trunked systems provide the only alternative for shared systems in many areas of the country. As mentioned, trunking provides the means for many virtual channels, used privately between defined users, from a relatively few radio frequencies. This allows multiple agencies to come together on a shared system, use common channels (talk groups), and still have private channels.

As public safety radio use migrated toward digital and trunked radio systems, the community saw a need—and an opportunity—to escape proprietary systems by setting future standards. Project 25 began in 1989 as a joint effort of the Association of Public-Safety Communications Officials – International (APCO) and the National Association of State Telecommunications Directors (NASTD) to ensure that public safety agencies would have an open, standards-based alternative for digital radio systems. Today, P25 provides that standard and extends into Phase II and Phase III to eliminate the lock-in that proprietary trunked systems face.[112]

112. For additional information on the P25 phases, see www.tiaonline.org/standards/technology/project_25/.

Department of Homeland Security Technical Assistance

The U.S. Department of Homeland Security offers help to recipients of its grants to improve interagency communications. Under guidance of the Office of Emergency Communications, the Interoperable Communications Technical Assistance Program (ICTAP) provides policy, operational, and technical help to projects funded under DHS programs.

See www.publicsafetytools.info.

Security

The security of public infrastructure, including information and communications systems, is of critical importance today. Security covers a much broader expanse than can be covered here, but we want to note issues that an interagency communications project manager may face. Particularly, there is a delicate balance between security and availability, which affects interoperability.

Traditional information technology (IT) systems have long been guided by formal, well-defined security practices. Radio system managers increasingly face the same threats as their traditional IT counterparts. For example, denial of service attacks can affect and spread to all IP-based systems. The very flexibility that drives greater use of VoIP also increases vulnerabilities. All radio system managers seeking to secure their systems should review the National Infrastructure Protection Plan (NIPP) and follow established IT security practices.

All radio system managers should review the NIPP and follow established IT security practices.

The National Institute of Standards and Technology (NIST) within the U.S. Department of Commerce published a series of documents on generally accepted security principles and practices.[113] These documents recommend controls for securing federal IT systems[114] and principles addressing the subject from a systems perspective.[115] Collectively, the series describes the means of building a suitable foundation for secure voice radio systems.

NIST addresses security throughout phases of the system life cycle:

1. Project initiation
2. Development and acquisition
3. Implementation
4. Operations and maintenance
5. Disposition of systems

The first four of these five phases of a system life cycle should be familiar to the reader from Part 2 of this book. NIST principles point out that technology security isn't added onto systems, but rather built into them from the foundation up.

SEARCH received funding from the COPS Office to produce a companion Tech Guide, *Law Enforcement Tech Guide on Information Technology Security: How to Assess Risk and Establish Effective Policies*. This guide provides more information on NIST security processes.

Advanced Radio Features for Physical Security

When most people think of radio systems security, they think of physically securing the infrastructure and logically securing the information that passes over the network. Conventional radio systems over the years have been plagued by the ease at which someone with malicious intent can disrupt communications by transmitting on the system. Lost and stolen radios are the biggest risk, but more than one system has been disrupted when a responder's young child wanted "to be like mommy or daddy" and spirited off a radio to the closet to talk.

NIST points out that security is built into systems from the ground up.

113. Marianne Swanson and Barbara Guttman, *Generally Accepted Principles and Practices for Securing Information Technology Systems* (Washington, D.C.: U.S. Department of Commerce, National Institute of Standards and Technology, September 1996). See http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf .

114. Ron Ross, et al., *Recommended Security Controls for Federal Information Systems*, NIST SP 800-53 (Washington, D.C.: U.S. Department of Commerce, National Institute of Standards and Technology, February 2005, including updates to June 17, 2005). See http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final.pdf.

115. Gary Stoneburner, Clark Hayden, and Alexis Feringa, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*, NIST SP 800-27 (Washington, D.C.: U.S. Department of Commerce, National Institute of Standards and Technology, June 2001). See http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf.

Trunked radio systems control access to channels centrally, so they offer an inherent ability to reject rogue radios with just a little effort on the system administrator's part. Better yet, modern radio systems, both conventional and trunked, offer the ability to disable the lost, stolen, or otherwise misappropriated radio remotely. That prevents the radio from requesting system access—or even transmitting at all!

Modern radio systems allow radios to be disabled remotely.

While physical security is understandable as a fundamental to securing all systems, securing the information the system is built to transport is another matter.

Encryption and Key Management

It's nearly impossible with current public safety technologies to prevent radio signals from being captured over the air. Military spread-spectrum techniques, where a signal is distributed across a wide swath of frequencies and thus made largely undetectable, haven't found their way to public safety voice systems. It's worthy to note that this technique is used with some cellular and wireless data systems, though.

Confidentiality, integrity, and availability are the three objectives of information security.

Encryption is the traditional means of securing voice radio communications since they are so easily intercepted. The three objectives of information security—**confidentiality**, **integrity**, and **availability**—are served to different degrees by encryption.

- *Confidentiality* of the information is expected as long as the encryption system is uncompromised and the keys for unlocking its secrets are secured.
- *Integrity* of the information is the assurance that what was received is what was sent by the original sender. Encryption provides this, to a degree, simply by locking up the data, but other parts of the system contribute to its integrity by limiting access to the system to authorized users.
- *Availability* is a particularly difficult feature to secure in the radio environment because channel access can be denied simply by the presence of a rogue transmitter spewing RF noise across the frequencies in use (denial of service).

The great majority of public safety voice communications don't require great confidentiality. From an interoperability perspective, encryption brings additional challenges. Not only do all users that are expected to talk together on secure channels have to use the same encryption means and methods, but they must have current keys to lock and unlock transmissions. In effect, encryption adds technological junction points where interagency communications can be fractured.

For example, most gateway approaches, such as console patches and other common audio bridges, require special care when moving traffic from one secure channel to another. There is the risk of originally encrypted traffic on one channel being decrypted at a gateway and broadcast unexpectedly on another channel unencrypted. Alternately, the encrypted traffic may be moved through a gateway to users of other channels who are unable to decrypt and use it, resulting in added noise and confusion for those users.

Encrypted interagency communications require greater efforts to ensure interoperability.

Despite these difficulties, the confidentiality and integrity of certain voice communications is of high value—high enough that availability risks are acceptable. Where needed, encrypted communications between multiple agencies require additional attention to technical compatibilities and their maintenance, to ensure interoperability.

☐ The Digital Future of Encryption

Encryption of analog radio communications has a checkered past. Users have long been dissatisfied with the reduced range of encrypted communications and the lack of techniques to deal with a harsh RF environment that confuses the encryption systems. Analog encryption has been a necessary evil in most cases.

Digital communications naturally support encryption.

Digital radios bring a new day, though. The digital radio signal is by nature encoded, which reduces casual reception by common FM scanning receivers. As digital scanners become more prevalent, there's another arrow in the public safety radio quiver: The digital signal can be encrypted without effect on the system's basic functionality. That is, the transmitters, receivers, and radio environment can keep on moving digital bits regardless of whether they're scrambled one way or another.

☐ Key Management

The big trick in dealing with encryption is managing the keys. Since encryption creates virtual private networks within the radio system, access to the keys allows users to be part of the network. There may be multiple sets of keys for different sets of users to limit access to only those with a pre-defined need for the "private" channel.

Like any other encryption system, those for radio are only as strong as their weakest link. That's usually the keys. Many an encryption system has been compromised because the secret decoder ring was stolen. Thankfully, this isn't a frequent occurrence with public safety radio systems, but all it takes is one radio to be lost or stolen for all others sharing the same keys to need re-keying.

First responder mobility challenges key management. If all users of an encrypted channel were in the same room, it would be easy to keep the keys up-to-date, switching them out as necessary to maintain security. Unfortunately for the radio system manager, users are rarely so easily contained. The need for "over the air re-keying" (OTAR) becomes apparent if you consider just the logistical challenge of maintaining encryption keys for potentially thousands of users on a large, modern radio system. OTAR is simply the process of encryption keys being passed from the system control point to affected radios, and then activated simultaneously.

OTAR is over the air re-keying, or updating encryption keys wirelessly.

OTAR makes it possible to load keys on the fly wherever the radios are, and then switch to the new set when they are all prepared.

Technology provides the means of key management in a shared radio system. The more difficult part is managing the people environment to gain concurrence about what will be encrypted, how the process and keys will be managed, and procedures for use of encrypted channels so users don't become stranded on yet another desert island lacking interagency communications. This aspect of the technology is managed as a piece of the larger puzzle addressed throughout this book.

Encryption is managed as a piece of the larger interoperability project.

☐ Reports Available from SAFECOM

The Public Safety Wireless Network (PSWN) Program produced two reports on encryption key management. These reports are available from the SAFECOM library. The first is an introductory text explaining basic encryption concepts.[116] The second provides a key management plan template.[117]

116. *Introduction to Encryption Key Management for Public Safety Radio Systems*, Public Safety Wireless Network Program, October 2001. See www.safecomprogram.gov/library/Lists/Library/Attachments/208/Security_Issues_and_Analysis_Report%20-%20Encryption_Key_Management.pdf.

117. *Key Management Plan Template for Public Safety Land Mobile Radio Systems*, Public Safety Wireless Network Program, February 2002. See www.safecomprogram.gov/library/Lists/Library/DispForm.aspx?ID=202.

On The Horizon – Voice Communications Technology

The most promising technology on the horizon for improving interoperability is software defined radios (SDR). Much like other electronics throughout the technology universe, radios are increasingly designed with internal functionality provided through software.

Thirty-five years ago, public safety radios were limited to just a few frequencies spread over a narrow slice of RF spectrum. Twenty-five years ago, early "programmable" radios were in use that allowed frequencies available in the radio to be changed electronically, rather than by substituting internal hardware. These radios also allowed use of a greater range of frequencies.

Over the past 25 years, more and more radio functionality has been moved from hardware to software. Software defined radios are the next evolution that will allow even greater agility not only across bands, but also with varying channel bandwidths and across different modes of transmission. For example, the U.S. Department of Defense is developing the Joint Tactical Radio System that will operate across multiple bands, use various analog and digital transmission modes, and provide a combined platform to eliminate a plethora of different systems.

It will take many years, decades even, for the existing disparate wireless systems to evolve and effectively converge with VoIP technologies. Recognizing the challenges ahead, the OEC developed "The Public Safety Communications Evolution" brochure as a tool to:[118]

- Educate the public safety community and elected and appointed officials about the future of emergency communications
- Describe the evolution of emergency communications and how traditional land mobile radio (LMR) communications used today may converge with wireless broadband in the future if specific requirements are met
- Discuss some of the most important requirements that must be met to achieve the desired long-term state of convergence

Similarly, different means of getting information through radio channels will become more flexible. Narrow and wider bandwidths will be accommodated through software, as will analog and a variety of digital transmission modes.

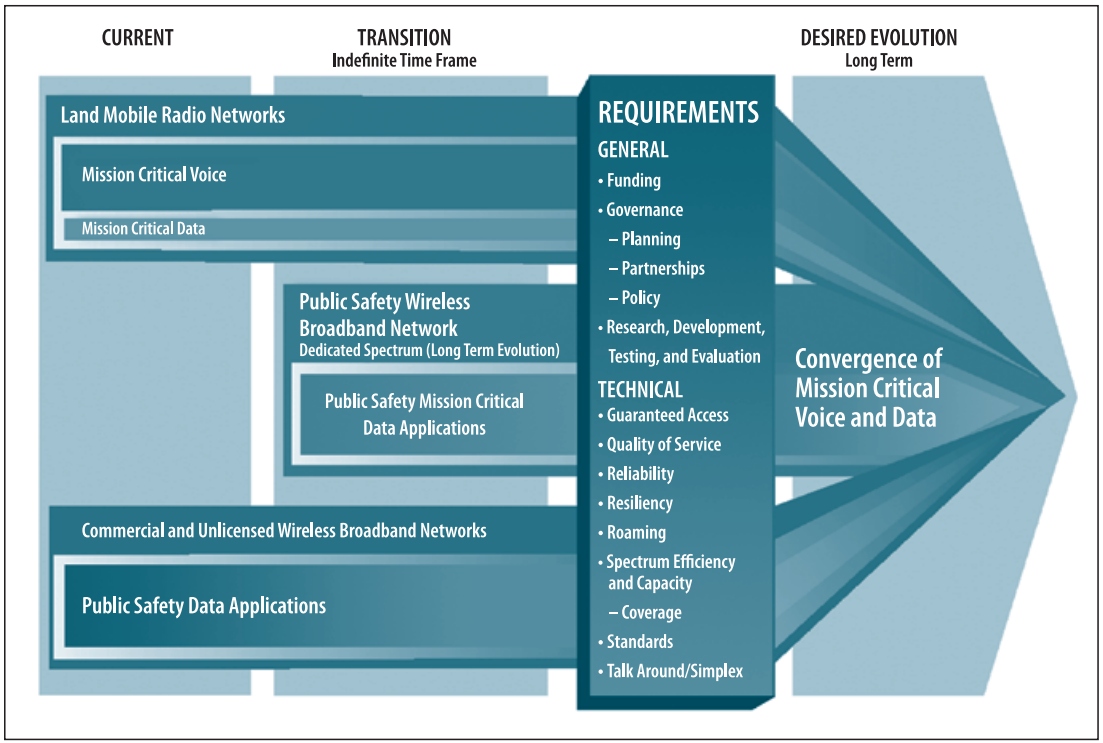
Today, Project 25 radios provide analog and digital, narrow and wider band capabilities largely through software. SDR technologies will gradually be integrated into mainstream public safety radios, eliminating some of the technological barriers preventing direct interagency communications.

Much like artificial intelligence in computer systems, SDR techniques will be embedded in technology and largely unobserved by the end user. The effects will be significant, however.

Technology marches on, bringing new capabilities and overcoming the old.

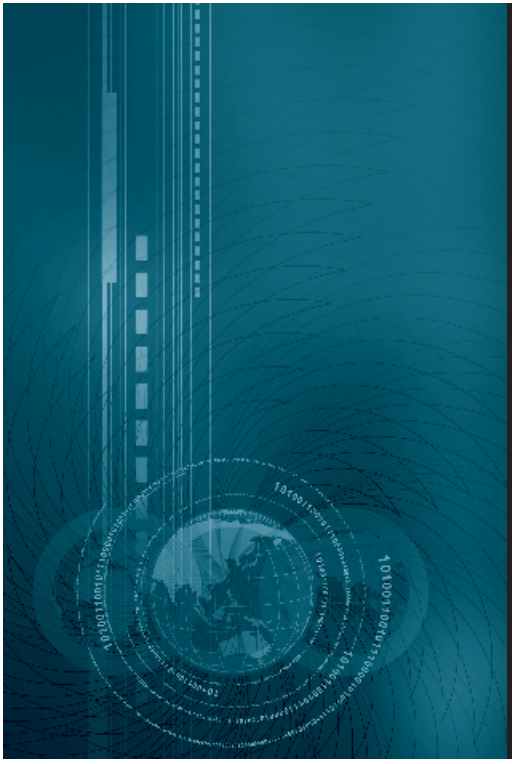
118. Download the brochure at **www.publicsafetytools.info/oec_guidance/start_oec_guidance.php**.

Figure 16-11: Public Safety Communications Evolution



Source: Public Safety Communications Evolution, November 2011. U.S. Department of Homeland Security. **www.publicsafetytools.info/oec_guidance/docs/Public_Safety_Communications_Evolution_Brochure.pdf**

Figure 16-11 illustrates a public safety communications evolution by describing the long-term transition toward a desired converged future.



CHAPTER 17

Data Communications

VOICE COMMUNICATIONS OVER RADIO IS ACCEPTED as the central interoperability challenge, but it's increasingly difficult to separate voice from data and wired from wireless networks. Data networks tie together public safety communications systems from beginning to end. From the automatic number identification/automatic location identification (ANI/ALI) data arriving with an initial 9-1-1 call for service through the responder's final status code transmission from a mobile data computer, data systems connect responders to the public they serve and beyond. Even at the core of modern radio systems, wired and wireless data networks connect dispatch consoles to central electronics banks, link complex subsystems in the radio room, and carry audio widely between distant transmitters.

SAFECOM Technology Library

The SAFECOM technology library is a prime source for information about data communications systems. It includes documents from multiple sources, including the past Public Safety Wireless Network (PSWN) Program. See www.safecomprogram.gov/library/default.aspx.

Since the World Wide Web surfaced from the primordial Internet more than 20 years ago, data networks have come to pervade our homes, our offices, and even our automobiles. In this chapter, we look first at the protocols and standards that fueled this explosive growth and then into the technologies of both wired and wireless data networks. We'll wrap up the chapter with an examination of how data networks are secured and close with a look at data communications developments on the horizon.

Common Protocols and Standards

Common protocols and standards are the building blocks for interoperability, technologically or otherwise. At technical and social levels, alike, the Internet has influenced the world of information sharing greatly, from civic and commercial realms, to government. Just as the World Wide Web evolved as the model of information sharing globally, the common protocols it was built upon have become the foundation for nearly all data communications.

Common protocols and standards are the building blocks for interoperability.

The Internetworking Effect

What suite of protocols powers the Internet and every private network that has arisen from it?

If the title of the next section doesn't give it away, you might be surprised to know it's the *Transmission Control Protocol/Internet Protocol* best known as TCP/IP. Lest the term "suite" strike you as pretty fancy for just two protocols, understand that TCP/IP is commonly used to refer to dozens of protocols that lace the Internet together.

The Internet has become so ubiquitous and part of our daily lives that we may forget at times that it's a minor miracle that we can transfer a wide assortment of data around the world with little worry about how it happens. Electronic mail, files, video, music, and now voice telephony speed from point to point across increasingly faster and faster networks upon an amazingly standardized set of protocols.

Internationally, a body known as the Internet Engineering Task Force (IETF)[119] is central to the definition and formalization of these protocols. It's beyond the scope of this Guide to get very deep into the protocols, but we do want to note that they are many, varied, and built upon one another. The most basic, hidden services of wired and wireless networks connect physical components together in standardized ways, while increasingly complex protocols are built upon them to deliver information in a humanly digestible form.

☐ At the Heart: TCP/IP and Friends

TCP/IP, its companions, and associated other protocols occupy the middle ground of a stack of open, standardized means of interconnecting information sources. The very term "Internet Protocol" describes the original purpose for the protocol: Connecting different networks.

Other key Internet protocols that have found their way into the heart of public safety communications include:

- **File Transfer Protocol (FTP) –** A venerable graybeard of the earliest days of internetworking and today underlying data transfer between many criminal records and other information sharing systems.
- **Simple Mail Transfer Protocol (SMTP)** and **Post Office Protocol Version 3 (POP3) –** Key pieces of today's e-mail, as well as automated fingerprint identification systems.
- **User Datagram Protocol (UDP) –** TCP's alter-ego and the foundation for Voice over IP (VoIP) networking, including systems for interconnecting radios over data networks.

119. The IETF is an international community of industry, academia, and government. See www.ietf.org/.

- **Session Initiation Protocol (SIP)** and **Real-time Transport Protocol (RTP)** – Doing yeoman's work for networking services as varied as peer-to-peer music sharing systems and VoIP telephony, beyond to the instant messaging capabilities of the Capital Wireless Integrated Network (CapWIN) around Washington, D.C.
- **Lightweight Directory Access Protocol (LDAP)** – Serving at the core of NASA's Integrated Services Environment just as it serves user authentication information to encryption engines securing Kansas' innovative Criminal Justice Information System.
- **Simple Network Management Protocol (SNMP)** – Giving technical staff a view into the core of the Internet, as well as the supervisory control and data acquisition systems of modern trunked radio systems.
- These and many more standardized protocols have brought about a Golden Age for data sharing at a technical level, whether those data packets are carrying criminal history records, voice dispatch communications, or fingerprint images. As much as they contribute, these networking protocols alone don't make the data intelligible, though. It takes higher-level application protocols and standards to transform data into information.

XML—Universal Language of the Internet

Broad adoption of Internet protocols has supported growth of a key tool for interoperable data communications: the Extensible Markup Language (XML). A project manager dealing with interagency data communications today will have a hard time avoiding XML. It is the universal language of data communications today, particularly for data that cross system and jurisdictional boundaries.

XML actually had its origin before widespread use of the Internet in something called *Standardized General Markup Language* (SGML). A markup language is basically simple, textual conventions for describing associated data and providing further details on how the data are used. SGML is actually an international standard; XML is a simplified subset of it.

XML's magic is in its extensibility—its innate capacity to describe and extend itself for wrapping data into ever more useful packages. It is structured text, making it both human and computer readable, but XML can wrap up and describe data of all types. Software capable of processing XML *documents*—packages of XML text and data payloads—are able to "learn" of the structure of the document, including associated non-textual data.

Applications that consume XML-based data can be structured to be very rigid or flexible in understanding the data. That is, the software can restrict itself to consuming only highly structured information or maintaining flexibility to learn how to deal with data in different forms. Not all systems can or should be so willing to adapt to changing data forms, particularly in high-security and mission-critical environments, but XML provides the means for software to extend its understanding of the data it processes as designers see fit.

☐ XML in the Justice System

As with consumer, business, and governmental systems worldwide, in recent years public safety information systems in the United States have become more open through the application of XML. Work by individuals and organizations involved with the justice system nationwide contributed key, anchor tenants to the information sharing bazaar—the Global Justice XML Data Model (GJXDM) and the National Information Exchange Model (NIEM).

There's no shortage of acronyms in the world of Internet protocols—even ones with others embedded!

The U.S. Department of Justice (DOJ), Office of Justice Programs (OJP), released the GJXDM in early 2004. Following the success of GJXDM, the DOJ and U.S. Department of Homeland Security established a partnership to broaden the scope of GJXDM beyond justice. This partnership resulted in the NIEM,[120] essentially an extension of GJXDM. NIEM is a comprehensive product that consists of a **data dictionary**, a **data model,** and several **XML schema**.

A data dictionary is a set of standardized descriptions of data to provide a common definition and means of describing, for example, a person's name. A data model expands on a data dictionary by establishing how different data elements relate to each other. For example, a person has a birth date, height, and weight, while a vehicle has a make, model, and style. An XML schema defines how data elements make up documents and how documents are related to each other. Remember that in the worldwide web of information protocols and standards, XML documents can range from very simple to very complex sets of information.

Simply put, NIEM provides a structured approach, a controlled vocabulary, and tools for achieving semantic interoperability in information exchanges. Where GJXDM was mainly focused on information sharing within the justice enterprise, NIEM supports information sharing across the enterprise of justice, public safety, emergency/disaster

120. See www.niem.gov.

management, intelligence, and homeland security. NIEM addresses the problem of individual agencies or jurisdictions using different terminology to describe the same thing, which has traditionally obstructed effective information exchange. NIEM allows these independent exchange partners to maintain control over their internal business processes (including terminology), while agreeing more easily on the terminology to use when they exchange information among themselves.

SEARCH has contributed greatly to the success of NIEM through active participation in NIEM governance, and development and implementation of NIEM conformant exchanges. SEARCH developed the Justice Information Exchange Modeling (JIEM) tool to facilitate development of information exchange specifications that use NIEM.[121] NIEM—and all the information sharing capabilities it has spawned—contribute greatly to interoperability for data communications. It can be a complicated subject, so for our purposes we'll leave the topic here and move on to how NIEM, and other uses of XML are advancing emergency response.

☐ XML in Emergency Response

The beauty of XML standardization efforts is that, with proper coordination, different areas of interest or domains can leverage each other's efforts. For example, the Law Enforcement Information Technology Standards Council (LEITSC) has established priority objectives for development of functional standards for records management and computer-aided dispatch systems. XML and related standards are the primary focus of its technical committee. These standards are also going to be very useful as information exchanges are developed for the implementation of Next Generation 9-1-1 (NG9-1-1).[122]

The Law Enforcement Information Technology Standards Council (LEITSC) website offers emerging CAD/RMS standards information: www.theiacp.org/Technology/OperationalTechnologies/CADRMS/tabid/831/Default.aspx.

The emergency management world is also seeing rapid growth of information sharing standards built around XML. For example, the Emergency Data Exchange Language (EDXL) is an effort to advance interoperability between data systems. EDXL is being developed through a practitioner-driven, public/private partnership between industry and the DHS's Disaster Management (DM) E-Gov (electronic government) initiative to advance U.S. disaster management response capabilities.

121. For more information on JIEM, see www.search.org/programs/info/jiem/.

122. For information about data exchanges, information sharing, and data interoperability, see www.ijis.org/docs/Guide_Info_Sharing_Data%20Interoperability_Local_Comm_Ctrs_FINAL.pdf and www.ijis.org/docs/Priority_Data_Exchanges_LocalCommCtrs_FINAL.pdf.

One standard established before DM involvement was the Common Alerting Protocol (CAP). EDXL is a broad suite of draft standards to provide tools for information sharing, while CAP is a specific, standardized protocol for alerting and event notification.[123]

The Disaster Management Interoperability Services (DMIS) are part of a Presidential e-government initiative to advance U.S. disaster management response capabilities.

CAP has seen use in both government-funded and commercial applications. Disaster Management Interoperability Services (DMIS),[124] an interoperability software toolset providing real-time, secure sharing of incident information for public safety agencies, is an example of the former. DHS funded development of it as part of the Disaster Management initiative. DMIS uses the CAP standard, as well as other XML-based exchanges, to move information between users of either a no-cost DMIS client application or with other applications capable of using the protocol. The DMIS client application provides basic functionality using standard, web-based services to create, view, and exchange incident information.

Commercially, crisis information management systems (CIMS) are a rapidly developing breed of application built for information sharing. They commonly use XML to push data to and pull it from other information systems. Distinct from traditional records management systems (RMS) and computer-aided dispatch (CAD) systems used by responder agencies, CIMS implementations are designed specifically to collect, distribute, and display information from various sources—both from humans and machines. For example, popular commercial products allow integration of information from CAD and geographic information systems (GIS), while providing document sharing, video conferencing, and other collaboration tools.

Commercial CIMS products with XML capabilities are finding popular adoption among emergency management officials for non-crisis events, too. For example:

- **Football Championship Game – Jacksonville, Florida**
  In February 2005, the Jacksonville Sheriff's Office used a commercial, web-based collaboration product to help it and dozens of other agencies manage information flowing in all directions. It was found to be particularly useful in maintaining situational awareness, executing Incident Command System (ICS) incident action plans, and producing situation reports.

123. For further information, see the Organization for the Advancement of Structured Information Standards (OASIS) website at www.oasis-open.org. OASIS is a not-for-profit consortium of vendors and users developing guidelines for interoperable systems. For information on EDXL, see http://xml.coverpages.org/edxl.html.

124. See the Disaster Management Interoperability Services website at www.cmi-services.org/.

- **Presidential Inauguration – Washington, D.C.**
  A month earlier, the Metropolitan Police Department in Washington, D.C., made use of a different CIMS to push information to other homeland security and law enforcement information systems. It also helped the department document activities for subsequent federal reimbursement of expenses.
- **National Political Convention – Boston, Massachusetts**
  Boston was the site for a national political convention late in the summer of 2004. The Boston Emergency Management Agency implemented yet a different commercial CIMS for hundreds of users across dozens of agencies and organizations. It was used for incident information sharing between the agency and the U.S. Environmental Protection Agency during the convention.

There is great room for XML and similar technologies to advance interoperability of data communications. An October 2004 report on CIMS interoperability by Dartmouth College[125] noted the need to create a common vocabulary of technical terms, define data elements, promote public/private partnerships to advance standards, and overcome "cultural issues" affecting information sharing. Similarly, standards for open messaging between RMS, CAD, and NG9-1-1[126] systems are in their infancy.

Building Blocks for Interoperability

The very process of standardizing, accepting, and implementing common protocols is endlessly challenging due to the rate of change in the world of information technology. Government, in general, and public safety, more specifically, faces these challenges in spades. It's impossible to adopt the power of standards without becoming part of the dynamic evolution of information sharing.

Challenges notwithstanding, the future looks bright for greater and greater technical capabilities to share data, make it intelligible, and, ultimately, make it into actionable information. Information sharing is the true measure of interoperability.

125. Institute for Security Technology Studies, *Crisis Information Management Software (CIMS) Interoperability: A Status Report,* Hanover, NH: Dartmouth College, October 2004. See www.ists.dartmouth.edu/library/213.pdf.

126. The migration to NG9-1-1 is being led by the U.S. Department of Transportation (US DOT). More information is available at http://transition.fcc.gov/pshs/services/911-services/nextgen.html and www.its.dot.gov/ng911/index.htm.

It's becoming increasingly difficult to separate wired and wireless modes of communications.

Common protocols and standards arising in conjunction with the Internet depend on physical networks to move data about. Increasingly, interagency communications capabilities are evolving simultaneously on both wired and wireless networks. In truth, it's becoming increasingly difficult to separate the two modes of communications. For the sake of discussing data communications technologies that use the protocols and standards mentioned, we'll take a look at wired and wireless networks separately.

Wired Data Networks

The term "network" is a very flexible one, something like "system." On the one hand, it's used formally to refer to technical assemblages of telecommunications hardware and software. On the other, it's used more broadly in reference to groups of people or functions linked by technology. Our use in this chapter is toward the technical side of that spread.

A Whole Lotta *AN Going On!

Most anyone who has been around an office computer environment more than about an hour has heard the term "local area network" (LAN). But have you heard about campus, metropolitan, and wide area networks? Despite the obvious fun that can be had by use of the acronyms (in some quarters, at least), do these have anything to do with communications interoperability?

Absolutely! Just as common terminology is a key factor for interoperability, the design and operation of interagency communications systems is furthered by common use and understanding of terms. Data networking is easier to understand with a common, consistent vocabulary for network types.

☐ Standard Network Types

Local area networks are typically constrained to an office or building environment. There are physical wiring limitations that have given rise to the term, but generally a LAN is considered a geographically and functionally constrained network connecting personal computers, and perhaps, servers and printers. In many cases, a LAN is no longer strictly a wired network; it can be a combination of wired and wireless connectivity and constrained by distance, business functionality, and security.

Multiple LANs may coexist in a single location to segregate use for functional or security purposes. For example, it's not uncommon in dispatch centers for separate connections to the state data network and to the city or county LAN to exist side-by-side—often connecting separate computers. The state connection provides access to the FBI's National Crime Information Center (NCIC), the National Law Enforcement Telecommunications System (NLETS), and state systems, while the other provides access to local applications and data.

Statewide networks connect local, campus, and metropolitan area networks to create the technical basis for law enforcement information sharing.

From an end user's point of view, campus (CAN), metropolitan (MAN), and wide area networks (WAN) may appear to be largely arbitrary distinctions in the geographic extent of data communications systems. To a large extent, that's true. Data networks are categorized in these geographic terms more for the sake of convenience in discussion rather than inherent technical limitations.

Groupings of networks to create successively larger ones are defined at a technical level, of course, but widespread adoption of TCP/IP for data communications often makes them seem all as part of a larger whole. With the right agreements, technicians, and overarching applications—such as the Internet—they can easily serve as the technical means of data communications interoperability.

The FBI's CJIS WAN connects law enforcement agencies nationwide.

For example, the FBI's Criminal Justice Information Systems (CJIS) WAN connects to each state and some larger cities, providing the backbone for a wide array of NCIC, criminal history, and automated fingerprint identification services to agencies nationwide. Network technicians can install specialized network equipment to make it possible to pass information over the Internet securely. CJIS information travels over the Internet on a virtual private network (VPN) and is encrypted for security. Increasingly, organizations are using message-layer approaches, such as Web Services Security (WS-Security), to secure information over the Internet (and other "unsecure" WANs) without incurring the expense and complexity of setting up VPNs. The Global Reference Architecture (GRA) offers detailed guidance on how to use WS-Security and the full set of web services standards for secure justice and public safety information exchanges.[127]

127. For information on GRA, see http://it.ojp.gov/default.aspx?area=nationalInitiatives&page=1015.

☐ Public Safety Network Types

Project MESA was an international effort to standardize broadband wireless access for emergency response and introduced several important networking concepts to public safety.[128] We'll discuss Project MESA further in the final section of this chapter, but want to introduce the networking concepts here.

In the process of examining intra- and interagency needs, different types of networks were defined to address differing needs for high-speed data exchange. These aren't necessarily independent networks and may, indeed, be built of similar technology. Each amounts to a separate *functional* type of network.

How many acronyms can fit on the head of a PAN?

The first is a personal area network (PAN). In public safety response, this is the networking environment that surrounds the individual responder. It may be short-range wireless means for microphones, location monitoring devices, and environmental sensors to be connected to a personal hub. From that hub, information may be made available to the individual responder, as it may be shared with team members, incident commanders, and beyond. The PAN will carry both data and voice communications within close proximity to the first responder.

At a higher level, an incident area network (IAN) links together multiple response elements responding to a particular incident. This is most easily seen as a network geographically limited to the scene of the incident, but the concept recognizes that outgoing and incoming communications from afar—such as from a central Emergency Operations Center (EOC)—may touch the incident area network as well.

Beyond individual incidents, the jurisdiction area network (JAN) describes functional and even technical networking requirements that span the general operational environment of one or more agencies. In essence, it serves to connect both widely dispersed resources and concentrated "hot spots."

The final networking type described by Project MESA is the extended area network (EAN). Multiple sub-networks linked across broad geographic expanses are most commonly known as wide area networks or extranets. The idea is that through use of common technical protocols, application-level interoperability, and shared security measures, data communications can span individual agency and jurisdictional networks.

128. See www.etsi.org/WebSite/AboutETSI/GlobalRole/MESA.aspx.

Data Networking Evolution

For law enforcement, all this network connectivity isn't that unusual. NCIC, NLETS, and other collaborative data systems have allowed agencies to share wanted persons, stolen vehicle, and other information nationwide for almost 45 years. What has changed is that the networks have gotten smarter, faster, and more flexible. Dedicated circuits between systems that were more than adequate for decades have largely been relegated to the dust bin of history, as more and more data needs to be moved between agencies.

☐ Speed Matters

Wired networks speeds have increased dramatically as the world has come to revolve more and more around access to information. Thirty-five years ago ARPANET, the Internet's precursor, was the private domain of military facilities, defense contractors, and a few universities. At that time LAN speeds were measured at just a few million binary digits (bits) per second—megabits per second or Mbps. WAN circuits speeds were orders of magnitude slower, running at what we would today consider good dial-up modem rates, measured in thousands of bits per second (kilobits/sec or Kbps).

Today, NCIC and NLETS rely primarily on packet-switched circuits.

Today, LANs are commonly built to transfer billions of bits per second (gigabits/sec or Gbps). Long-haul fiber optic circuits forming the backbones of modern WANs are measured in hundreds of Mbps, while even home access to the Internet is often measured in broadband terms of megabits per second. From 2005 to 2010, home Internet access in the United States via broadband connections increased from 60 to 95.1 percent.[129]

☐ Intelligent Networks

"The days of the fat, dumb pipe, are over."

According to industry sources,[130] increasing demand for TCP/IP networks to carry great volumes of data of various types brings a need for more smarts than raw bandwidth. Traditionally, demand for smarter networks arises as co-workers or collaborators get spread further apart geographically, depend more and more on web- and other server-based applications, and increasingly depend on IP networks for carrying voice and other multimedia traffic. Internetworking of government functions is at an all-time high, and is more critical as information sharing is not only expected by the public, but demanded.

129. Source: www.websiteoptimization.com/bw/1002/.

130. Leon Erlanger, "Building the intelligent network," *InfoWorld*, July 18, 2005. See www.infoworld.com/reports/29SRintelnet.html.

Network intelligence has gradually come to the public safety world. Fifteen years ago, essentially all access to NLETS and NCIC occurred over circuit-switched connections using specialized network protocols. Today, the majority occurs over packet-switched circuits, most typically using TCP/IP at the core. While private virtual circuits are used to protect traffic from prying, the circuits are still "virtual"; that is, they're passing through a larger cloud of intermingled bits and bytes.

☐ Improving Quality of Service

VoIP applications need "fast" networks.

The greatest driving factor for increased network intelligence today for public safety purposes is to provide an improved quality of service (QoS) at a low networking level to applications, such as VoIP telephony. VoIP has improved considerably over the years; however, there may be some latency from network delays. Digitized and packetized audio from telephones or radios that is being sent and received in real time demands fast networks. Delays measured in fractions of a second can disable the simultaneous two-way (duplex) voice communications that we're used to with telephones.

And fast isn't the same as big, though the two have been intertwined since the earliest days of networking. That big, fat networking pipe connecting two points might, like a railroad, be capable of carrying huge amounts of data, but it can be slow to get up to speed and equally slow to decelerate, like a train. In the networking world—wired or wireless—delays between transmission and receipt of bits and bytes is referred to as latency.

Network latency affects duplex (simultaneous two-way) communications.

Have you ever noticed how hard it can be to carry on a cellular telephone conversation when there are network delays between you and the other party? Estimates are that delays of more than a quarter of a second (250 milliseconds) disrupt the normal flow of human conversations. Even that tiny amount of time serves as a cue for the wetware between our ears to switch from "receiving" to "transmitting" in a two-way conversation.

Wired data networks are more easily managed to maintain a set QoS level than are wireless networks.

Wired Networks Keep On Keeping On

Thankfully, the interoperability of data communications over wired connections isn't much of a technical challenge today. From the physical level of wiring through widely accepted and reliable networking protocols, there's little to prevent network architects from lacing together interagency communications systems.

The greater challenges probably come from *too* much connectivity, which brings security concerns, fosters the spread of viruses and other network pestilence, and generally threatens the manageability of segmented networks. We will address security issues and technologies associated with data communications later in this chapter.

Wireless Data Networks

Many protocols originally developed for wired data networks have migrated to wireless networks. While most originally arose for connecting independent data networks that were built at the time from coax cable and twisted pairs of copper wire, the rapidly evolving wireless world is pouring its own share of protocols into a spreading pool.

Higher level standards and protocols, such as IP, are equally as important in wireless networks as they are elsewhere. However, unlike in the wired world, there is great variance in low-level wireless standards. For example, Ethernet[131] in its various speeds is widely accepted and used for wiring together LANs using standard types of cabling. The wireless data world is much more in a state of transition, by comparison.

In this section, we'll look at wireless data communications technologies available to public safety agencies for their own networks and those used for commercial services. We'll tour the field in this order:

- Common Principles
- Private Radio Technologies
- Commercial Radio Technologies
- Wireless Local Area Networking
- Wireless Metropolitan Area Networking

We'll conclude this section with a look at how to evaluate options for building your own wireless data networks versus buying services from commercial providers.

131. *Ethernet* is the popular name given to wired networking technology that has grown dominant over the past 35 years. Technically, it is standardized by the Institute of Electrical and Electronic Engineers (IEEE) as IEEE 802.3. It has evolved in speed over the years, with good backwards compatibility.

Common Principles

In your own considerations of wireless data communications technology, work to avoid "Silver Bulletitis"—an affliction leading to the belief that there's a single, ideal technology awaiting discovery or deployment that will provide interoperability. Keep in mind a few common principles demonstrating the practical realities and tradeoffs facing network architects.

☐ Speed, Capacity, and Throughput are Interrelated

Speed, capacity, and throughput (the effective amount of data passed) are all interrelated. All other factors being equal, more users on a network reduces total, practical capacity. This occurs because each user brings a certain amount of networking overhead. Theoretically, with enough users, a network would reach capacity with overhead communications alone, and provide no useful capacity for practical applications. More users reduce the amount of network bandwidth available to all, reducing throughput and effective speed.

☐ Faster and Deeper Requires Smaller "Cells"

Recognize that basic networking theory maintains that more, smaller zones of coverage (e.g., cells and hot spots) provide greater speed and capacity. The tradeoff is complexity and cost. A side benefit is that smaller cells of coverage result in greater overlap, on a proportional basis, and thus redundancy.

Wireless WANs that depend on few fixed access points for bringing mobile users back home are relatively limited in capacity and speed. This applies to satellite networks, as well. Satellite data networking also demonstrates that the mere distance between users and central network components limits speed and capacity. That is, nature decrees that electromagnetic radiation is going to take a fixed amount of time to travel a given distance. Wireless networks of a few hundred feet in radius are faster and offer the potential for greater capacity than those connecting hundreds or thousands of miles into space.

☐ Advanced Capabilities Cost Money

Speed, coverage, reliability, and security cost money. Compromises are made continuously in public and private sector data networking, as well as by commercial carriers, to provide the most for the best price. What constitutes an acceptable compromise and a good price varies widely, of course.

There's no free lunch, only relative compromises.

Private Radio Technologies

Early generation technologies available for wireless data systems were slow, providing speed only adequate for low-volume textual information. Very much like other data systems that relied on wide-area coverage by a relatively few transmitters, early mobile data systems ran at 4.8, 9.6, and 19.2 Kbps—rates considered painfully slow even by dial-up networking standards today. And recognize that those systems weren't dedicated to a single, point-to-point connection as a dial-up modem is, but shared each frequency among multiple users, just as voice radio channels were used.

As a matter of fact, the technologies for these systems operated in standard voice channels, encoding data as sounds just like a telephone modem does. Technological advancements allowed data speeds to double and then double again, but the result was still a network that ran a poor second compared to dial-up. Did we mention the data channel was shared by multiple users?

Slow technologies are still in wide use. The most common mobile data technologies in public safety use today still only run at 19.2 Kbps. And digital voice radios don't offer any immediate improvement. Project 25 (P25) radios, capable of passing voice and data digitally, have a maximum rate of 9.6 Kbps and effective throughput of half that.

Mobile data systems built to operate across voice channels are inevitably constrained by the channel width of those frequencies. Greater bandwidth yields greater speed. Data systems built upon the narrow bandwidth of existing voice channels are limited to low speeds.

Wideband standards for public safety use are rapidly developing. We'll take a look at the prognosis for them in the final section of this chapter, "On the Horizon."

Microwave Subsystems

Many public safety voice and data systems have private microwave backbones linking together facilities and radio sites. While unlicensed microwave technology is widely available, most agencies prefer to build backbone networks using microwave channels assigned by certified frequency coordinators and licensed through the FCC. As with voice frequencies, coordination and FCC licensing offers much better assurances that agencies won't suddenly find other users interfering with their operations.

Microwave backbone networks are popular because they offer high-speed, high-bandwidth connections without requirements for intervening infrastructure or recurring payments to network carriers for leased lines. Properly engineered, they are also considered more resilient to accidental and intentional disruptions.

(More than one public safety network has been subject to "backhoe fade," the tongue-in-cheek term for accidental breaks of buried wire and fiber circuits. Anyone involved in telecommunications for long has a horror story to tell of losing network access, receiving a call from a network carrier, and eventually gasping in awe at the sight of thousands of wires ripped apart by an errant backhoe operator.)

Shared microwave backbones are increasingly popular among public safety agencies looking to leverage funds and take advantage of the tremendous capacity of today's microwave systems. They are a natural adjunct to other shared systems, offering great potential to interconnect parts of participating agencies' data, voice radio, and telephone systems.

Commercial Radio Technologies

Industry sources estimate that carriers providing wireless data services at dial-up speeds or better cover 98.49 percent of the U.S. population. More than 50 percent of the population is covered by systems offering high-speed data transfer ranging from 10 to 30 times dial-up rates.[132] The lure of such speed and implied capacity is understandable. Across the country, more and more agencies have turned to commercial services.

Commercial wireless services long ago outran technologies commonly available to public safety agencies for their own systems—at least in terms of raw speed and capacity. Recognizing that agency choices may value availability over raw performance, the attraction of commercial data rates is often a deciding factor.

132. See footnote 124.

☐ Background: Generations of Commercial Wireless Services

Wireless data services provided by commercial carriers are commonly discussed in terms of which "generation" they're part of. There's some debate about what exactly splits the generations (sound familiar?), but we know that for wireless data communications, it tends to be based on transfer rates—or the amount of data measured in thousands or millions of bits per second (Kbps or Mbps).

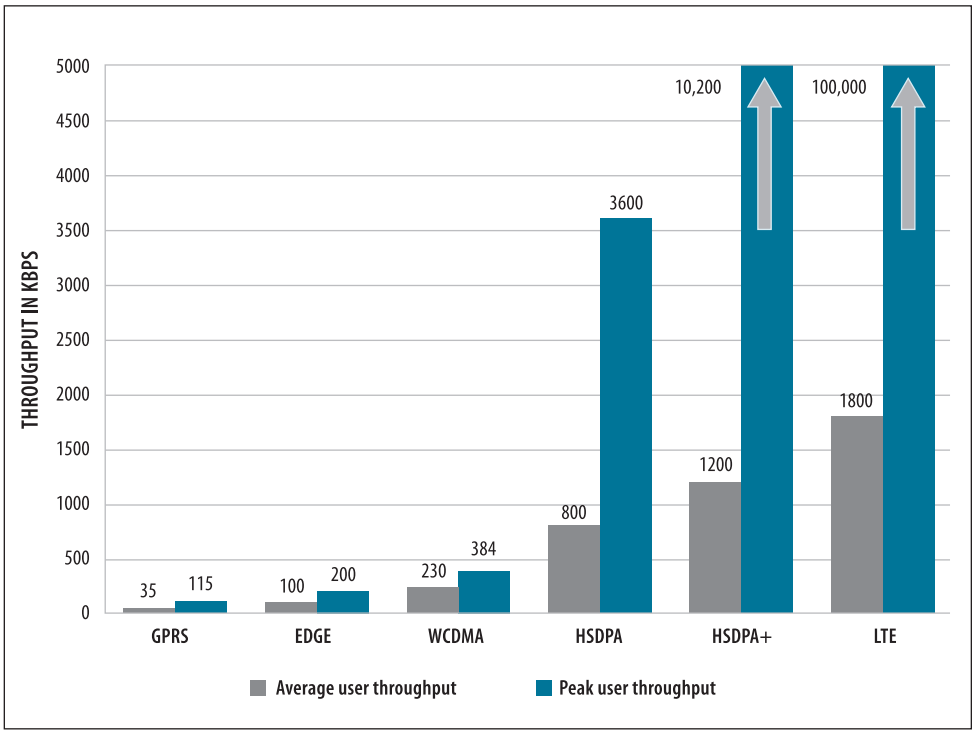
At the time of this writing, commercial wireless service providers are offering third and fourth generation services (3G and 4G).

A brief taxonomy and short chronology of commercial wireless services may be useful.[133]

- **1G –** Defined only in retrospect, first generation wireless services included early analog cellular telephones and overlay data services, such as Cellular Digital Packet Data (CDPD). CDPD was popular among police and fire agencies as a commercial networking alternative. It ran at 19.2 kilobits/second (Kbps).
- **2G –** Digital cellular telephone systems are considered the second generation. Second generation systems include GSM, iDEN, and cdmaOne. Data rates for these technologies are around 20 Kbps.
- **2.5G –** Services running in the range of a few dozen to a few hundred Kbps are considered to be in this transitional ground from dial-up speeds to wideband, 3G services. Examples include GPRS, 1xRTT, and EDGE technologies.
- **3G –** High-speed technologies that can compete with wired services, ranging in speed from a few hundred Kbps to more than 1 Mbps. Examples include EvDO and UMTS.
- **4G –** Uses technology considered more efficient and can exchange data at 100 Mbit/sec. 4G is expected to enable pervasive computing which would allow simultaneous connections to multiple high-speed networks. Examples include LTE and WiMax.

133. The world of wireless data networking is full of acronyms. See Appendix F for a glossary of terms.

Figure 17-1: Peak and Average Throughput Per User With Technology Evolution



Source: ATIC Consulting

☐ Growing Private and Public Sector Use

Use of commercial wireless services continues to grow. A 2004 report by the Yankee Group, a high technology market research firm, indicated that more than half of large U.S. businesses would be using wireless wide area networks by mid-2006, citing the growth of 3G networks and their capacity to bring enterprise-class application services to the mobile user.[134]

Figure 17-1 depicts real-world data throughput of different wireless technologies and likely dates for broad availability.

Technologically, public safety tends to trail, but track, private data networking trends. We can look at those broader trends to project where public safety wireless is headed.

134. Eugene Signorini, *3G Represents an Inflection Point for Enterprise Mobility*, Boston, MA: Yankee Group Research, Inc., 2004.

A late 2005 reader survey by *Mission Critical Communications*[135] showed that slightly more than half of respondents said that traditional, private radio networks were the primary means of wireless data access for their agencies' responders, while more than a third relied on commercial networks. Significantly, about half as many respondent agencies relied on high-speed wireless LAN (WLAN) technologies as relied on commercial services—16 percent versus 34 percent.

As of 2012, WLAN interoperability is still relevant for a large percentage of public safety agencies.

The use of popular WLAN technologies is an interesting parallel of public safety and private sector uses. The cited survey also indicated that 75 percent of respondent agencies planned to deploy WLANs at their facilities before the end of 2007. Of course, there's a difference between using the technology at facilities, such as offices and parking garages, and covering the wide, deep emergency response environ. Due to the limited range of WLANs, most agencies using them rely on traditional private or commercial networks for more general coverage.

Wireless Local Area Networks

The growth and popularity of wireless local area networks is indisputable. Various industry sources cite double-digit annual increase rates for the equipment market and triple digit growth rates in the number of users worldwide. The value of mobile computing long recognized by public safety agencies has now been recognized in the consumer, industry, and general business sectors. Popularity has driven down the technology's price and spurred innovation in its use.

Satellite Services

Commercial satellite services are the only means for U.S. public safety agencies to gain the advantages of space-based communications.

As addressed in Chapter 16, **Voice Communications**, satellites have a definite niche for emergency response. They also have technical and cost drawbacks that keep terrestrial data networks as the first choice, where available.

☐ WLAN Technologies

As a matter of background, wireless LAN technologies are most often described in terms of the standards they employ. The most common is the IEEE 802.11 family of standards,[136] which define wireless networks very similar to the Ethernet (IEEE 802.3) in the wired world.

135. "Public Safety Report: Snapshot Survey – Wireless Networking," *MissionCritical Communications*, September 2005, p. 64.

136. For further technical information on the IEEE 802.11 series of standards, see www.ieee802.org/11/.

The Wi-Fi Alliance brought a standard implementation to 802.11 wireless networks.

Standardization has been key to WLAN growth. However, it wasn't until the thorny issue of interoperability was taken up that manufacturers adopted a common implementation of the standards, fueling an explosion in growth. The Wi-Fi Alliance, a nonprofit trade association established late in the 1990s, brought that common implementation well known today as *Wireless Fidelity* or Wi-Fi.[137] The term *Wi-Fi* has become such a standard part of the international wireless lexicon that it's well to remember it has a formal meaning.

High-speed wireless data networks are an important part of the interoperability equation. As agencies seek greater mobile access to information and weigh their options to rent or own networks providing it, the value of wireless data networking technologies is being factored in. We will address those technologies and evaluate privately owned versus commercially available options shortly.

☐ Wi-Fi and Other 802.11 Networks

The IEEE 802.11 series of standards covers two incompatible types of technology: 802.11a and 802.11b. Though very similar technologically and both serving well in accurately described Wi-Fi networks, a key difference is in the frequency bands they use. Just like voice technology, WLANs using different frequency bands lack technical interoperability at a very low level. It's possible to include both 802.11a and b technologies in the same box, but they're still operating independently even if linked at a higher networking level.

802.11a networks use 5.8 GHz frequencies, while 802.11b networks use 2.4 GHz.

Both 802.11a and b technologies operate in the FCC's unlicensed frequency bands at 5.8 and 2.4 GHz, respectively. While use of these bands is unlicensed, it is regulated and every WLAN device has to comply. Antenna and power emission regulations limit what can be done with the devices.

Largely due to the more limited range of the frequencies used, 802.11a has not been as widely adopted as 802.11b, despite its higher data rates. As a matter of fact, common reference to Wi-Fi hotspots—local access points or base stations with broader network connections—in public transit areas and cyber cafés is usually referring to the slower, lower frequency equipment. Less range means that more access points are needed to cover the same area, leading to higher costs and greater complexity in linking all the devices together to a common backbone.

137. Wi-Fi® is a registered trademark of the Wi-Fi Alliance. Wi-Fi CERTIFIED™ equipment is the implementation standard for the vast majority of WLANs. See www.wi-fi.org.

Frequency Hopping Spread Spectrum

Hedy Lamarr

In the midst of World War II, communications security was paramount. A little-known patent was filed in 1941 by "H. K. Markey et al."—Hedy K. Markey, better known to the world as the actress Hedy Lamarr—for a system using frequency hopping spread spectrum techniques to code transmissions for radio-guided torpedoes.

Now known to be a particularly robust transmission mode and effective encoding method, spread spectrum techniques never found popularity until long after Patent No. 2,292,387, "Secret Communications System," expired. Lamarr lived to see their popularization in military and commercial technologies.

Offering the lower frequency (2.4 GHz) and high data rates (up to 54 Mbps), 802.11g was amended to 802.11n in 2009. This improved the previous 802.11 standards by adding multiple-input multiple-output antennas (MIMO). 802.11n operates on both the 2.4 GHz and the lesser used 5 GHz bands. It has a maximum net data rate of 600 Mbps and enhanced security features. 802.11n is backwardly compatible to all 802.11 versions. Real throughput is still less than half of the raw data rate and just like 802.11a and b, this latest Wi-Fi technology throttles itself back when faced with interference or weak signals in order to maintain connections.

Outside of these factors, the 802.11 wireless networks are very similar in operation. Each uses very few wideband channels in their respective bands. They move bits of data around the wide channel in a predetermined sequence to improve throughput and resistance to certain types of interference. This process of *direct-sequence spread spectrum* (DSSS) is common to Wi-Fi technologies.

By contrast, the basic 802.11 standard also provides for frequency hopping spread spectrum (FHSS) techniques that operate at lower data rates (1 or 2 Mbps), but which in application offer greater resistance to signal jamming and interference, unintentional or otherwise. Wireless network technologies using 802.11 FHSS are available for public safety use, though are eclipsed by the Wi-Fi juggernaut.

Wireless Data Networking Standards

The world of wireless standards is wide. Primary data networking standards are established by the IEEE in its 802 series, including:

802.11 – The ubiquitous wireless LAN standards. Wi-Fi equipment and networks are a particular, popular implementation of the IEEE 802.11 standards. Actual TCP/IP throughput is about half of the raw channel rate, which itself is stepped down to maintain connections in weaker coverage areas.

- **802.11a –** Operating at 5.8 GHz, offering up to 54 Mbps raw data rates
- **802.11b –** Operating at 2.4 GHz, offering up to 11 Mbps raw data rates
- **802.11g –** Operating at 2.4 GHz, offering up to 54 Mbps raw data rates and backwardly compatible with 802.11b
- **802.11n –** Operating at 2.4 GHz, offering up to 600 Mbps raw data rates, backwardly compatible with all 802.11 versions and enhanced security

Other **802.11** standards define further implementation details, such as:

- **802.11i –** A 2004 amendment correcting early security vulnerabilities in the Wired Equivalent Privacy (WEP) specification. A subset of this standard was adopted by industry and entitled Wi-Fi Protected Access™ (WPA).

And next generation technologies are on the horizon, as well.

The first, **802.11ac**, operates in the same frequency bands as today's wireless networks and therefore should be backward compatible. It calls for much higher speeds (up to almost 7 Gbps) compared to today's top speeds of 300–450 Mbps.

The second, **802.11ad**, also calls for wireless networking to approximately 7 Gbps. However, the 802.11ad standard is being written for operation at approximately 60 GHz.

802.15 – Standards under development for personal area networks (PANs).

802.16d and e – Developing wireless metropolitan area network (WMAN) standards for faster wireless networks promising greater range and security. Where 802.11 equipment is technically related to its Ethernet forebears, 802.16 is different at a low level, so is fundamentally incompatible with WLAN technologies. 802.16e is intended to bring enhancements for mobile access to the networks. The interoperable standard for 802.16 implementations is referred to as WiMAX.

802.20 – Another WMAN standards effort intended to provide broadband wireless access for true vehicular speeds. Formally known as the Mobile Broadband Wireless Access, this standards process is in its early stages. It's expected to be years before compliant equipment is commercially available.

☐ WLAN Interoperability

There's a remarkable degree of interoperability with Wi-Fi, making it such a popular technology. A combination of de jure (IEEE) and de facto (Wi-Fi Alliance) standards, openly accessible radio spectrum, and a receptive market caused it to boom. Manufacturers rushed to meet market demand, which in turn brought competitive prices for buyers. It's easy today to pick up a Wi-Fi network access card for less than the monthly cost of a cell phone and use it to connect to the Internet from public access points, often at no cost.

Some public safety WLAN needs can and have been met by no more sophisticated equipment than used by the average cyber café surfer. For example, "parking lot LANs" have been created and police vehicles suitably equipped so that reports, virus software updates, and other sizeable packages of data can be transferred in a reasonable amount of time when the officer gets within range of the station hotspot.

☐ WLAN Weaknesses

The beauty of 802.11 wireless LANs is that the technology is readily available and highly developed due to its popularity. However, the technology does have a number of weaknesses.

- **Popularity.** Yep, the strength is also a weakness. Wi-Fi (IEEE 802.11b) hotspots today all compete for the same few slices of 2.4 GHz radio spectrum. Separate networks can operate in the same slice and over the same territory, but physics dictates that they will interfere with one another.
- **Use of unlicensed spectrum.** Popularity is one thing, but unlicensed use of the spectrum makes the WLAN ecosystem a bit of a jungle. Other widespread public, commercial, and industrial use of both 2.4 and 5.8 GHz unlicensed spectrum reduces its suitability for public safety purposes. For example, Wi-Fi networks share the band with cordless phones, microwave ovens, and nanny cams.
- **Security.** Wi-Fi networks have gotten a bit of a black eye for their hack-ability. While this has led public safety agencies toward proprietary adaptations of 802.11 standards, it seemingly hasn't dampened general enthusiasm elsewhere. Network security experts point out that all shared-medium networks, such as basic Ethernet and Wi-Fi, are inherently more vulnerable. Encryption and other security measures have been used for years with wired and wireless networks, alike, to at least protect the privacy of their communications.

- **Mobility.** The 802.11 standard suite wasn't designed for mobile devices that may be moving rapidly in and out of optimal coverage or in and out of range of different network access points. In essence, each Wi-Fi cell is a separate LAN unto itself, using separate network addresses. Even if the WLAN could manage breaking and making connections each time a user moved from one cell to another, IP-based networks and applications don't deal well with addresses being switched on the fly, potentially several times a minute or more when users operate at cell boundaries. Proprietary extensions to 802.11 standards reduce this to a degree by making the access points "dumb" and moving most intelligence for managing mobility back to the network core. This comes at the cost of less standardization and, somewhat as a result, less interoperability.

802.11n – Operates in the 2.4 GHz and 5 GHz bands, offers up to 600 Mbps raw data rates, is backwardly compatible with all 802.11 versions and provides enhanced security.
On the horizon, the first 802.11ac – Operates in the same frequency bands as today's wireless networks. It calls for much higher speeds (up to almost 7 Gbps) compared to today's top speeds of 300–450 Mbps.

WLAN Technology in Action

Across the United States, municipalities are building wireless LANs to serve their residents, businesses, visitors, and agencies. Large and small cities, alike, see wireless as a means to bridge the "digital divide"—which keeps less advantaged citizens from the wealth of information and services available in our Connected Age—as well as a means to serve the community broadly. Almost exclusively, Wi-Fi technology is being used to deliver wireless access to users.

Examples are numerous. "Wireless Philadelphia" and San Francisco's "TechConnect" are two of the most expansive initiatives. The City of Philadelphia requested proposals in early 2005 looking for a network to cover its 135 square miles.[138] Later the same year, the City and County of San Francisco followed suit in efforts to cover its 49 square miles. Each specified Wi-Fi, specifically 802.11b or g, recognizing—as put by San Francisco—"its ubiquity in user devices, standardization, low cost and ease of provisioning."[139]

Spokane, Newark, and many other jurisdictions across the country are using WLAN technologies to provide broadband data to emergency responders.

Large cities are not the only ones building wireless LAN systems. Police and other emergency agencies across the country are already making use of the technology, if at smaller scales, to connect field staff to information. Examples include Spokane, Washington, which has built a dual-use network with separate segments for public access and emergency agency use, and the Newark (New Jersey) Police Department, which used a COPS Office Interoperable Communications Technology Program grant to install a broadband wireless network linking multiple policing partners and hospitals around the area.

138. The Wireless Philadelphia website has further information. See www.wirelessphiladelphia.net/.

139. The San Francisco TechConnect website has further information. See www.sfgov.org/site/tech_connect_page.asp?id=33899.

In essence and practice, these are standards-based, shared systems. Widely available and compatible technology provides agencies using Wi-Fi networks with a competitive market to keep prices down and service quality up. Broad use outside the public safety market brings innovation and further economies of scale through sharing of infrastructure. Police, fire, and EMS agencies are leveraging the commercial popularity of Wi-Fi technology.

Multiagency Wi-Fi networks provide standards-based, shared data communications systems.

☐ Mesh Networking Technologies

Many of the networks mentioned above will be built in the form of *mesh networks*, a form of networking that links together individual nodes to blanket part or all of a jurisdiction with broadband wireless access while providing high reliability and system throughput. According to ABI Research, implementation of citywide wireless networks were expected to be the largest factor in the growth of mesh networks between 2005 and 2010.[140]

The term "mesh network" has come to be used rather loosely in recent years, but properly refers to a network of many nodes, each of which communicates with two or more of its neighboring nodes. End-user network devices, such as a mobile data computer, can access a mesh network and thereby become part of it, but rarely are designed to be part of the mesh fabric, itself.

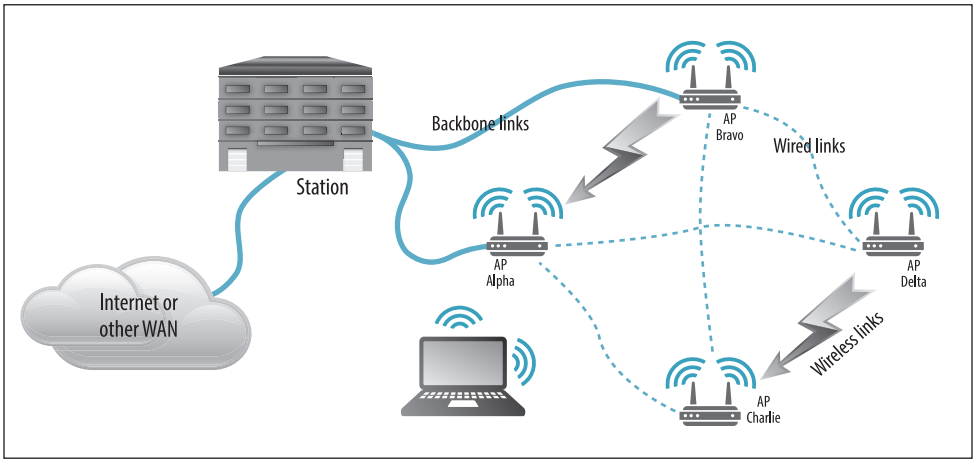
A mesh network is made up of many nodes, each communicating with two or more others.

Figure 17-2 on page 344 depicts a simple mesh network of four access points that communicate with each other and mobile computers. Each access point (AP) maintains a line of communications with all other APs. Traffic received at one AP is passed to the station and, potentially, on to a wide area network (WAN) either directly or through another access point.

Wired or wireless links separate from the WLAN channels provide alternative paths for the traffic to follow. This helps in balancing traffic on the mesh links and provides resiliency in case one of the intermediate APs is lost. Circuits or links that carry masses of traffic from one point to another are referred to as backbone links.

140. "Mesh Network Market May See Tenfold Growth in Five Years," ABI Research press release, November 16, 2005. See also www.abiresearch.com/abiprdisplay.jsp?pressid=556.

Figure 17-2: Mesh Networking of WLAN Access Points



Mesh networks commonly use proprietary technologies to link Wi-Fi access points into a common network.

Consider an example. The laptop in Figure 17-2 is depicted as being able to communicate with either AP Alpha or Charlie. This assumes the APs have some share of overlapping coverage, which is common in real-world networks. Under normal conditions, Alpha would serve as the AP of choice since it's closer to the station, network-wise. If it went down for some reason, communications from the laptop could continue through Charlie to Bravo and onto the backbone.

This is a classic, full mesh network. If the individual APs weren't connected to all others, it would be considered a partial mesh. If each was linked directly back to the station, it wouldn't properly be called a mesh, but rather said to have a star network topology.

Mesh networking is becoming the rule rather than the exception when multitudes of WLAN access points are used in concert across a jurisdiction. WLANs linked together to metropolitan area networks (MANs) today require proprietary technologies to make them appear to users on both the wireless and wired sides as part of a single network. Not to draw too fine a point, but wireless mesh networking is a bit of a frontier itself. As of late 2005, there were no fewer than six companies offering different technologies to bridge WLANs into a common mesh.

While a lack of standards in this realm may cause interoperability concerns, it should be pointed out that the mesh technology is linking together parts in the background, not at the network level the user sees. In the networks discussed here, any common Wi-Fi enabled laptop computer could, with appropriate authorization, roam onto the mesh network, find the appropriate channel, and operate regardless of who manufactured the computer or its wireless card.

Wireless local area networks are an increasingly important means of interagency communications. The standardization, popularization, and widespread availability of Wi-Fi technology, in particular, has opened many broadband wireless opportunities for public safety agencies.

Rent or Own?

WLAN technology is one of several choices available for interagency data communications. Where public safety agencies had only one practical means of connecting mobile users to data sources—building their own networks—an explosion in commercial services has provided viable alternatives for many. With the popularization of consumer wireless data technologies, agencies now have a third, hybrid alternative to build their own networks from technology broadly available outside of the public safety environment.

We've heard heated debates about why one approach to wireless data for public safety agencies is preferable. There are many strong points to be made on either side, but ultimately, the best decision is made by agencies that put technological debates to simmer on the back burner while letting their own *business needs* drive the decision. Those needs and all compromises made will only then properly include consideration of system life cycle costs, security needs, and operational priorities.

There's no single right choice of wireless technologies. The techniques recommended in this Guide for managing interagency communications projects will lead to the best choice between wireless data technologies for your agencies' particular needs.

The chart in Figure 17-3 on pages 347–348 will be useful in balancing needs. Three alternatives are examined:

1. **Build Using Specialized Public Safety Technologies –** Traditionally, wireless data networks used by public safety agencies have been built by the agencies themselves, using niche technologies. Broad consumer and business use of the technologies never existed. Traditional, low-speed mobile data networks are included in this category.
2. **Lease Commercial Services –** Data network services are leased through a wireless carrier.
3. **Build Using Broadly Available Technologies –** Use of widespread wireless data technologies brings a hybrid option to build agency-owned networks from commonly available parts. Wireless LAN technologies are included in this category.[141]

In 2009, the FCC crafted the National Broadband Plan (NBP) as the roadmap to bring broadband to the United States, including to public safety.[142] The Nationwide Public Safety Broadband Network (NPSBN) contemplated in the NBP will serve as a new alternative.

In February 2012, Congress passed and President Obama signed the Middle Class Tax Relief and Job Creation Act (PL 112-96) into law. This legislation addressed several questions regarding spectrum, governance, and funding laying the foundation to develop and implement the NPSBN. The First Responder Network Authority (FirstNet) is responsible for taking "all actions necessary" to build, deploy, and operate the network, in consultation with federal, state, tribal, and local public safety stakeholders.[143] Stakeholders made substantial progress in 2012-2013, however, plans for the NPSBN are still maturing and initiatives for implementing the NPSBN are ongoing.

Pros and cons for decision factors and alternatives are provided. The "ratings" indicators include a minus sign (–) for detracting factors, a plus sign (+) for attractive factors, and a check mark (✔) for acceptable compromises.

141. As decisions are made regarding nationwide broadband, other alternatives may be added to this list.

142. For more information on this initiative and a copy of the NBP, see www.fcc.gov/broadband and www.broadband.gov/plan/.

143. FirstNet is an independent entity within the Department of Commerce's National Telecommunications and Information Administration and is the authority for the NPSBN. The President's National Security Telecommunications Advisory Committee, *NTSAC Nationwide Public Safety Broadband Network Scoping Report,* May 15, 2012, www.ncs.gov/nstac/reports/2012-05-15%20NPBSN%20Scoping%20Report.pdf.

Wireless Data Communications Rent or Own Decision Factors

Figure 17-3: Rent or Own Alternatives and Factors

— = Detracting Factors + = Attractive Factors ✓ = Acceptable Compromises

	SPEED			AVAILABILITY			RELIABILITY		
	Rating	Pro	Con	Rating	Pro	Con	Rating	Pro	Con
Build Using Specialized Public Safety Technologies	—	No nosebleeds	Data speeds at 1% to 5% of alternatives; improved coding techniques and software yield little relative improvement	+	Coverage designed for agency requirements	Design, construction, and implementation of networks takes time	+	Stable, dependable technologies built for the rigors of public safety use	Capacity is very low relative to alternatives and difficult to increase significantly
Lease Commercial Services	+	The fastest wide-area alternatives are available soonest	Technology turnover brings new user equipment and installation costs	—	Existing networks means systems can be brought up more quickly	Coverage is designed for broader market needs; reduced coverage in rural and isolated urban areas	—	Highest capacity, typically, due to sharing with other users	Capacity is designed for broader market needs; reduced capacity in rural and isolated urban areas; ruggedized user equipment may be required at higher cost
Build Using Broadly Available Technologies	✓	Much faster than traditional, specialized public safety technologies	Turnover of consumer and industry technologies is faster than specialized technologies traditionally used by public safety	✓	Coverage designed for agency requirements	Design, construction, and implementation of networks takes time; coverage is typically spotty compared to traditional networks; wide area coverage is expensive	✓	Capacity designed for agency requirements that can be increased relatively easily	High capacity to meet surge needs requires overbuilding; ruggedized user equipment may be required at higher cost

You'll note that the third alternative, building agency-owned networks from widely used technologies, is considered here a good compromise across the board. It is an increasingly attractive alternative buoyed by a boom in wireless data usage by consumers, business, and industry. Public safety usage was once a large share of the wireless data market, but today is miniscule by comparison. The advantages of long product life cycles and security through obscurity of traditional mobile data technologies are fading.

Figure 17-3: Rent or Own Alternatives and Factors *(continued)*

SECURITY			SUPPORT			COSTS		
Rating	Pro	Con	Rating	Pro	Con	Rating	Pro	Con
✓	Relatively obscure technologies lead to a bit more security	Staples of modern network security, such as Virtual Private Networks (VPNs) and advanced authentication, are difficult or impossible to use	—	Relative reliability of equipment leads to reduced support needs	Heavy reliance on vendors for information, even with internal support		Easily predictable initial costs; long product lifecycles	Limited market for the technology increases initial costs; ongoing maintenance costs can be high, mainly for vendor maintenance contracts, licenses, internal labor, and contracted services
✓	Broadband provides IP and other standards supporting modern network security measures	Common use and widely available information on technologies used increases vulnerabilities	+	Least amount of internal support required; broad usage means there is widely available community support	Lack of internal expertise and support leads to vendor dependence		Predictable costs that may be negotiated and contracted; lowest internal labor costs; other markets find wide-area commercial services cost-effective	Recurring costs, typically monthly; shortest lifecycles for user equipment; most rapid migration of technologies, adding to costs
✓	Broadband provides IP and other standards supporting modern network security measures	Widely available information on technologies used increases vulnerabilities	✓	Wide range of community support	Internal expertise requires continuous study; commercial user technologies are less rugged		Wide availability of technology reduces purchase, operations, and maintenance costs	Ongoing maintenance costs can be high, mainly for labor or services; relatively rapid equipment lifecycles

Cost factors vary by implementation. Initial and ongoing costs should be evaluated over comparable system lifecycles and assessed based on requirements met. Absolute dependence on any one or more requirements may lead to acceptance of higher costs.

☐ Leveraging Advantages: Layered Networks

Modern networking technology makes it possible, at a price, to combine the advantages of each of these approaches. The ideal is the coverage availability and reliability of traditional public safety wireless data networks combined with the speed, capacity, and suitability for advanced security measures that are supported by commercial services—and, of course, ideally available at the lowest cost over all systems' life cycles.

It is possible to build user devices making use of high-speed WLANs or hot spots, when available, switching to broader coverage, slower MANs between hot spots, and eventually resorting to low-speed WANs as the lowest common denominator. Practically speaking, this requires different radio technology at the lowest levels for each type of network, plus mobile equipment that dynamically chooses the ideal route for each packet of data. That route not only varies by location, but by the speed of the mobile device and other service demands on the broader networks.

The technology to do this is available today. Its use in supporting interagency communications needs is evolving. Networks upon networks are built to serve different needs and practical realities. Since the data networking is almost always provided through core infrastructure—as opposed to directly between units—the wider network, itself, serves as an ever-present gateway to other networks. With adoption of standard wireless and higher-level protocols, such as IP, security and our ability to manage it to serve interagency communications needs become key factors.

Ubiquitous, broadband wireless coverage is economically unfeasible in many jurisdictions. Narrowband, slow-speed data is often the only means to fill in gaps left in higher speed, higher bandwidth, shorter range WLANs.

Security

Security for data communications networks, wired and wireless alike, necessarily evolves at least as rapidly as the connecting technologies themselves. Threats have grown in direct proportion to the capacity and extent of networks stretching across the globe and deep into societies worldwide. Not only has access to networks by those with malicious and criminal intent grown tremendously, but every insecure networked computer can serve as a naïve accomplice in attacks. Growth in high-speed, always-on connections to homes and small businesses has magnified the risk.

It's easy to maintain secure data communications. Just lock up all computers networked together into a single room, building, or compound, secured electromagnetically to TEMPEST standards,[144] and then control physical access by their users. It's done all the time. It just isn't very practical for the public safety environment, particularly where interagency collaboration is the rule rather than the exception.

144. TEMPEST is a national standard defining limits of unintentional electromagnetic emissions from electronics for security purposes. Endorsed TEMPEST products are required for the most secure telecommunications networks, but are rarely specified for public safety purposes. See also www.nsa.gov/.

Interoperability requires the technical capability to share information within the legitimate constraints of each partner's security needs.

Police, fire, and EMS agencies maintaining their own physical or logical networks within or connected to others necessarily have security interests that must be maintained. Some, such as the FBI's Criminal Justice Information Systems (CJIS) Security Policy, are conditions of connecting to other networks. The boundaries between networks, physical and logical, are secured to control access, determine authorities, and provide means of auditing use. Interoperability requires the technical capability to share information within the legitimate constraints of each partner's security needs.

Whether to guard against criminal, terrorist, or nuisance attacks, network security tools continue to grow in sophistication and availability. We will examine some of those tools and their relations to interoperability in a moment. First, let's take a look at a key federal policy shaping law enforcement information systems.

FBI Criminal Justice Information Systems Security Policy

The CJIS Security Policy covers a number of security areas. Those related to interagency data communications are addressed here.

The FBI's National Crime Information Center (NCIC), the original information sharing system for law enforcement agencies, has brought changing needs for data communications security over the past 45 years. As central information repositories, NCIC and its younger siblings such as the Integrated Automated Fingerprint Identification System (IAFIS) originally operated over dedicated, point-to-point communications networks. These systems still connect state and local law enforcement agencies over commercial circuits segregated electronically and logically from other users, but today connect to other networks that are, themselves, widely connected elsewhere. Growing internetworking of all forms has shaped the FBI's Criminal Justice Information Services (CJIS) Security Policy.

☐ Scope

Established in 1999, the CJIS Security Policy affects all agencies using FBI systems managed by its CJIS Division. Because the policy is considered *Sensitive But Unclassified*, we'll only cite a couple of elements in passing. State and local agency systems connected to CJIS Division systems are required to adhere to the policy, so affected agencies should have ready access to it through official channels.

Most law enforcement agencies access NCIC and other similar systems through state-level proxies. *CJIS System Agencies* are those agencies with direct connections to CJIS Division systems. Most operate both as primary users of the systems and as intermediaries. For example, a state police computer center may be the termination point for a CJIS Division network circuit and, from a relative perspective, the start of a statewide data network for access by its own users and those of other agencies.

The CJIS Security Policy affects all agencies using FBI systems managed by its CJIS Division.

For both network and information security purposes, the CJIS Security Policy applies to all users of CJIS Division systems and the information produced by the system. Systems and networks not connected to the FBI aren't subject to the policy, but combined networks carrying CJIS, CAD, internal records, and radio system control traffic are increasingly common in law enforcement agencies.

☐ Technical Security Requirements

The CJIS Security Policy establishes standard requirements for technical security of connected systems. They include:

- Documentation of network configurations
- Use and maintenance of physically secure facilities
- Use of advanced authentication means
- Unique identifiers for all authenticated users
- Standards for network security, including:
  - Encryption and its management
  - Internet, wireless, and dial-up access
  - Firewalls
  - Audit trails
  - Virus protection
  - Penetration testing

A full treatment of these subjects is beyond the scope of this Guide; CJIS Security Policy, itself, is the definitive statement. The FBI CJIS Division and each CJIS System Agency has a designated Information Security Officer (ISO). Check with the ISO responsible for your agency with questions about requirements for data networks carrying CJIS Division information.

Since interagency communications can be affected by these requirements, we want to address a few from the standpoint of interoperability. A couple of basic principles of the CJIS Security Policy should be kept in mind for that discussion.

1. Different technical security requirements exist for public or shared networks than for those entirely under the control of a criminal justice agency. Networks with components in non-secure locations or which pass through public network segments require special authentication and encryption measures.
2. The 5 years from September 30, 2005 to September 30, 2010 was a transitional period for CJIS security requirements. Systems purchased or upgraded after the earlier date are subject to higher user authentication and encryption requirements. After the later date, all systems accessed from non-secure locations or across public network segments must meet the higher requirements.

In essence, the distinction between secure and non-secure locations and networks revolves around management control. Systems and networks entirely under the control of a criminal justice agency are considered secure. General governmental networks, the Internet, and telephone dial-up access are all examples of non-secure networks presumed more susceptible to compromise by unauthorized individuals.

☐ Interoperability

New connections between, for example, two local agency systems already subject to the policy don't necessarily bring added security requirements. However, interconnections made across networks managed by others likely do need additional security measures.

For example, consider a county sheriff's office and a municipal police department that are independent users of a state criminal justice network that provides their NCIC access. Each is subject to relevant parts of the CJIS Security Policy. If the two agencies chose to connect their internal, secure networks to share CJIS information over a general-use municipal or county government network, that connection would be subject to the same CJIS security requirements. This might occur if the two agencies wanted to exchange calls for service between their respective CAD systems that contain NCIC records information. The solution would be to secure the connection across the noncriminal justice network according to CJIS Security Policy, for example, by using a *virtual private network* (VPN) "tunnel" between the agencies.

Wireless data networks are given special treatment by the policy due to the ease by which RF signals can be intercepted. While encryption and security requirements are significant and must be observed on wireless networks of affected agencies, the practical effect of the policy on interagency data communications is the same, whether wired or wireless. This is because the interconnection of two wireless networks operated under the policy is handled just like the example above. Similarly, a single wireless network shared by multiple agencies, some CJIS users and some not (e.g., by police, fire, and EMS), must have its CJIS traffic encrypted and authenticated just as it would have to be over the Internet or other common-use network—say through the use of a VPN.

Wireless data networks are given special treatment by the CJIS Security Policy.

The process of operating interagency data networks brings challenges due, in large part, to the added coordination needed between agencies for common management of encryption and advanced authentication. It's simply harder for multiple agencies to coordinate management of the complex technologies, sharing control and authority. This is true in any multiagency security process; it's not a unique effect of the CJIS Security Policy.

Securing interagency data networks is more of a management than a technical challenge.

If information sharing is the product of interoperability, then FBI CJIS Division systems are a cornerstone of the process. From a data communications standpoint, the common need of criminal justice agencies nationwide to uphold the CJIS Security Policy means its provisions are a de facto standard. The FBI's longstanding Advisory Policy Board (APB) guides policy, assuring it meets federal, state, tribal, and local security requirements.

Common conventions, standards, and means of interfacing systems provide for interoperability of data communications. However, greater security requires more coordination and planning to assure interoperability, otherwise mechanisms to prevent unauthorized access can be barriers between those who would otherwise cooperate. For example, encryption will deny information access to anyone without the keys, seeking to use it illegitimately or just without adequate prior coordination.

Fortunately, the CJIS Security Policy is maintained and managed in part to provide this very coordination.

Securing Data Networks

Standard technologies for securing data networks are equally applicable to public safety. The primary tools of the trade are virtual private networks and firewalls. Both bring interoperability implications since their whole purpose is to restrict access.

☐ Virtual Private Networks

Virtual private networks are a workhorse of modern data communications security because they provide the means to secure a substream of data across a more broadly used network. The name alone pretty well describes their purpose.

VPNs can be implemented in hardware, software, or most commonly through a combination of both.

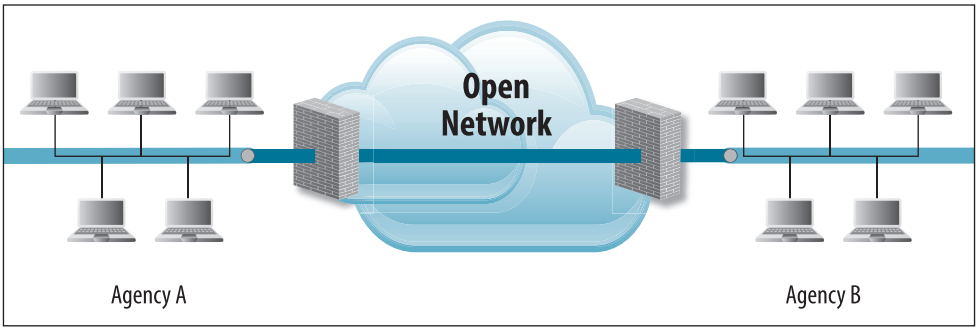
VPNs can be implemented in software, hardware, or most commonly through a combination of both. They are used over many different types of data networks, too. Physically, all types of wired and wireless networks are supported, most typically using Internet Protocol (IP) standards that are largely oblivious by design at this level to the type of physical connection or media they're running over.

The important issue from an interagency data communications standpoint (the topic of this chapter!) is mainly the "V" part of VPN—their virtual nature. Much as with trunked radio systems and their talk groups, a VPN is a virtual channel within a larger network. Granted, the "P" part (private) may be important or even critical to the virtual channel (network) users, but if so, that's probably true whether or not interagency communications are being carried.

In attempting to understand VPNs, it's useful to picture a tunnel between two networks through a third. For our simple purposes, picture two relatively secure, agency-operated networks using the Internet or common-use municipal network to hook up. Properly implemented, the secured border crossing points between each agency and the common network can be connected by a tunnel that looks open from either end, but inaccessible from the middle. See Figure 17-4 on page 355.

Advanced authentication techniques are generally used with VPNs. The techniques assure that the VPN only gets connected for authenticated users. Typically, a combination of a password and encryption certificate stored on the computer or in a device that can be connected to the computer serve to prove that a legitimate access attempt is being made. As with the VPN software, hardware configurations, and system permissions, user authentication has to be managed to provide interoperability across jointly connected data networks. The alternatives are undesirable: either no access or networks with big security holes in them.

Figure 17-4: VPN Tunnel Between Agency LANs



☐ Firewalls

The device at each network border depicted in Figure 17-4 is a firewall. A firewall is simply a device that sits at the junction point between two or more networks. This diagram is a bit of a simplification because there is typically more networking equipment, but recognize that the firewalls are the means to control traffic crossing network borders.

Firewalls can vary greatly in complexity and cost. They also can provide an endpoint for VPN connections.

The simplest firewall is a small computer with two network interfaces and software controlling what passes in which direction. Firewalls grow in complexity, up to enterprise-grade devices that may have dozens of physical networks attached and allow tens of thousands of individually encrypted VPN sessions.

And this brings us back to the point of interoperability. For purposes of interagency communications, firewalls can be an impediment. Most assuredly, they are a basic building block for secure data networks, but they can and do impede interagency communications if not managed to provide the capability.

An example of how firewalls are used may be helpful in understanding the interoperability impact. Consider the two agency LANs in Figure 17-4, each with its own firewalls. The firewalls are configured to block LAN file server and printer traffic from passing, while allowing Simple Mail Transfer Protocol (SMTP) connections to pass packaged fingerprint images.

Firewalls are typically configured to deny all traffic passing from the "untrusted" outside network to the "trusted" inside.

Before being activated, firewalls are loaded with rules defining what data may pass in which direction. For security purposes, they are typically configured to deny everything by default from the "untrusted" outside network to the "trusted" inside. Akin to Mikey in a classic breakfast cereal commercial, they don't like anything and refuse to pass it. One-by-one, specific rules are added to customize the firewall. As may be imagined, the firewall has to be configured accordingly to provide the needed interagency communications, in our case, without opening up the connected networks to all forms of virulence and pestilence.

Obviously, this takes coordination between network uses on either side as well as a degree of trust. It's not uncommon for two secure networks to be connected with firewalls back-to-back—one being managed by each of the agencies and likely sharing similar security profiles and traffic rules (in reverse). While this may seem like a waste of a good firewall, the fact of the matter is that it allows each party in the arrangement to control its own border, just like nations do with their own physical borders.

☐ Other Network Security Devices

Security has to be carefully managed to avoid it acting as a barrier to interoperability.

Network security is an important, dynamic field. A multitude of techniques and tools are used to protect individual and multiagency networks. Other tools include active *intrusion prevention systems* and more passive *intrusion detection systems*.

Any network subsystem that has the potential to shut down communications has an interoperability dimension. Whether through the security of VPNs, firewalls, or other subsystems, the intended communications can only proceed reliably if agency needs are clearly identified, articulated, and documented to assure the technology serves its purposes. Security doesn't need to be compromised to allow agencies to share information, but it has to be carefully managed to avoid it acting as a barrier.

On The Horizon

Rapidly developing technologies and standards mean that public safety agencies have greater and greater data networking capabilities to look forward to. The most exciting developments (and interest) has been in wireless networking.

WiMAX is the popular name for 802.16 wireless metropolitan area network implementations standards.

Wireless Metropolitan Area Networks

Standards development organizations in the United States and worldwide are working to tame the latest wireless frontier: High-speed data networks spanning greater distance, supporting truly mobile users who may move through and across cells of coverage at vehicular speeds consuming bandwidth at rates previously unseen. Wireless Metropolitan Area Networks (WMANs) are the current frontlines in standards development.

The term "WMAN" implies more expansive networks and this is, indeed, the intent of standards developed for them. In 1999, the IEEE formed its 802.16 Working Group on Broadband Wireless Access Standards. The series of standards, known as WiMax, defines faster, more robust broadband wireless access techniques that extend current wireless LAN technologies.[145]

The first WiMAX standard is for fixed point-to-point wireless networks.

The first WMAN standards released defined how fixed points are linked together with compliant technology. Other standards in the series that are under development provide definition for mobile uses, particularly intending to overcome Wi-Fi limitations.

In 2001, the WiMAX Forum was created by interested industry parties to bring common implementations of the diverse set of options within 802.16 standards, commonly known today as WiMAX.[146]

The 4.9 GHz frequency band was allocated by the FCC for exclusive public safety use.

Broadband Wireless Access for Public Safety

Public safety agencies have adapted commercial and popular use technologies to get broadband (multi-megabit per second) wireless networking in the past. Increased availability of commercial and unlicensed spectrum today brings the Internet wirelessly to the public. The power of mass markets and broad standards increasingly bear on police, fire, and EMS needs for broadband wireless services.

145. For more information, see www.ieee802.org/16/.

146. The WiMAX Forum is a nonprofit association formed by manufacturers to ensure interoperability of IEEE 802.16-compliant equipment and networks. See www.wimaxforum.org.

In 2002, the FCC allocated 50 MHz of spectrum in the 4.9 GHz band for public safety use.[147] The amount and location of the spectrum were important because they allow for the development of broadband wireless equipment to meet public safety needs for ruggedness and reliability, but which could be largely based on more popular commercial technologies, bringing economies of scale to keep costs low. For example, 802.11a Wi-Fi operates in the nearby 5.8 GHz band. With minor changes, popular consumer and industrial technology can be adapted to operate in the exclusive public safety band, offering greater security and reducing competition for the airwaves.

WLANs in the 4.9 GHz band will require more access points for the same coverage as 802.11b Wi-Fi networks.

In practice, 802.11a-based WLANs require much more infrastructure, such as wireless access points, than do 802.11b/g/n ones. This is due to the transmission characteristics of the different frequency bands used—5.8 v. 2.4 GHz.

How much of a difference in coverage is there? Studies show that the lower frequency signals are 100 to 1,000 times stronger in foliage, 10 to 100 times stronger through common building materials, and 5 to 10 times stronger filling in gaps in the open beyond the line-of-sight of transmitters.[148] Optimistic estimates are that twice as many access points are needed at the higher frequencies to provide the same level of coverage, while less optimistic ones suggest 5 to 10 times as many are needed.

Public safety agencies have built jurisdiction area networks (JANs) in the 4.9 GHz band using mesh and other networking topologies, but it's likely the technology will continue to be used mostly for campus and incident area networks in the near term.

The 700 MHz band offers some hope for dedicated public safety wireless broadband. The band was transitioned to public safety use as incumbent broadcasters moved to digital television (DTV) technologies. FCC regulations[149] originally allocated 120 paired channels (base and mobile), each 50 kHz wide, for wideband data systems. In 2007, the FCC amended its rules, reorganizing the band and folding this spectrum into a 10 MHz allocation for broadband systems. It subsequently licensed the 10 MHz for nationwide use to the Public Safety Spectrum Trust, a non-profit organization with a board of directors from national public safety organizations.

147. For further information on the FCC's actions, see "Public Safety's New Allocation – Answering Users' Questions on the 4.9 Gigahertz Band," available from SAFECOM at www.safecomprogram.gov/library/Lists/Library/Attachments/212/Public_Safetys_New_Allocation.pdf.

148. Daniel M. Dobkin, *RF Engineering for Wireless Networks: Hardware, Antennas, and Propagation*, Burlington, MA: Newnes, 2004.

149. 47 CFR Chapter I, § 90.533(c).

National Public Safety Telecommunications Council (NPSTC)

The NPSTC is a federation of public safety organizations. It is very active in wireless regulatory matters, standards development, and support for statewide interoperability committees.

In 2009, the National Public Safety Telecommunications Council (NPSTC) convened the 700 MHz Broadband Task Force to identify interoperability requirements for this spectrum.[150] The FCC incorporated most recommendations into waivers the following year, allowing 22 jurisdictions to enter into agreements with the Public Safety Spectrum Trust to use the spectrum for broadband wireless systems. Seven waiver recipients received $382M in federal Broadband Technology Opportunity (BTOP) grants for their projects.[151] In April 2012—to help agencies avoid investments incompatible with the nationwide network—the NTIA advised the BTOP waiver recipients to hold off on infrastructure deployment until FirstNet drafts the blueprint for the NPSBN architecture.[152] Almost a year later, in February 2013, FirstNet passed a resolution recommending NTIA lift the fund suspensions and allow BTOP grant recipients to move forward with approved projects.[153]

150. The Broadband Task Force final report is available online at www.npstc.org/download.jsp?tableId=37&column=217&id=10&file=700_MHz_BBTF_Final_Report_0090904_v1_1.pdf target=.

151. BTOP grants were authorized by American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009).

152. www.fiercebroadbandwireless.com/story/public-safety-told-stop-early-lte-deployments/2012-04-13#ixzz290XK0W.

153. www.ntia.doc.gov/other-publication/2013/02122013-firstnet-board-meeting-documents.

Project MESA

Now closed, Project MESA provided standard implementation profiles for public safety use of commercially available broadband wireless technology, much as the Wi-Fi Alliance and WiMAX Forum serve, rather than technology standards.

Project MESA, also known as the Public Safety Partnership, began as another in the Association of Public-Safety Communications Officials (APCO) International's respected series of projects shaping the world of public safety communications. As Project 25 proceeded to define the standard for public safety digital voice communications, an ambitious project to do the same for data began life as APCO Project 34 in 1995. Interest in the effort grew, eventually becoming international in scope. During a series of meetings in Mesa, Arizona, it was adopted as a joint project of the North American-based TIA and the European Telecommunications Standards Institute (ETSI). It became known as Project MESA.[154]

Project MESA sought to address both operability and interoperability aspects of broadband wireless data for public safety. Much like Project 25, resultant standards affected communications within and between agencies. However, unlike P25 it did not result in the production of new types of electronics and low-level engineering protocols.

Where public safety makes up a sizeable share of the two-way wireless voice world, its use of wireless data is increasingly insubstantial as a share of the total. Public safety agencies increasingly use more generalized commercial technologies for wireless data networking due to relatively gigantic leaps in capabilities being made available and dramatically dropping costs of equipment sold in great volumes. Broadband public safety networks will be built of generally commercialized electronics, customized at high network protocol layers for its unique needs.

Rich technical standards provide enough options that divergent implementations can preclude interoperability.

Standards: A Necessary, But Insufficient Condition

Late into this Guide, it probably comes as no surprise that we're advocates of standards for everything from training to technology. The wireless communications world has demonstrated particularly well how standards—particularly complex technological standards—are the first step toward interoperability. However, we've learned with Project 25, as the broader world has learned through WLAN implementations, that the plethora of options available under reasonable standards leads to divergent implementations of the technologies—and a lack of interoperability.

154. See www.projectmesa.org.

The Wi-Fi Alliance and WiMAX Forum previously mentioned were formed expressly to bring interoperability for implementations of IEEE 802.11 and 802.16 standard technologies, respectively. Early WLAN products operating well within IEEE 802.11 standards were not interoperable between manufacturers.

The WLAN market didn't take off until the Wi-Fi Alliance created a "meta-standard" narrowing the range of implementation options for 802.11 technologies and a process to certify Wi-Fi compatible products. As expected, this process brought critical mass to the market. Today, Wi-Fi, with all its compromises that reduce options across a well-considered standard, is being used around the world from coffee shop hotspots to public safety mesh networks.

Wireless LANs didn't take off until a subset of 802.11 standards was settled on.

The WiMAX Forum was created with forethought to assure interoperability. The success of those efforts in bringing broad standardization to WMAN implementations is yet to be seen, but the market is bound to be further advanced through them than it would have been otherwise.

In the public safety arena, debate continues in the digital voice realm about which elements of the broad set of P25 standards (TIA/EIA-102) must be implemented for interoperability. And because P25 is frequency-band agnostic, even use of its fundamental standard—the Common Air Interface—doesn't guarantee radios can talk to each other if they're operating in different bands. We expect similar interoperability questions to be raised in implementation of TIA-902 wideband standards for public safety data communications. Development of conformance tests is key to the practical use of both voice and data standards.

P25 (TIA/EIA-102) is a rich set of standards that can be interpreted and implemented in different ways.

This important debate can't be done adequate justice here, but suffice it to say that broad standards alone are not sufficient to guarantee interoperability in the technical realm. Further implementation standards are inevitable.

Epilogue

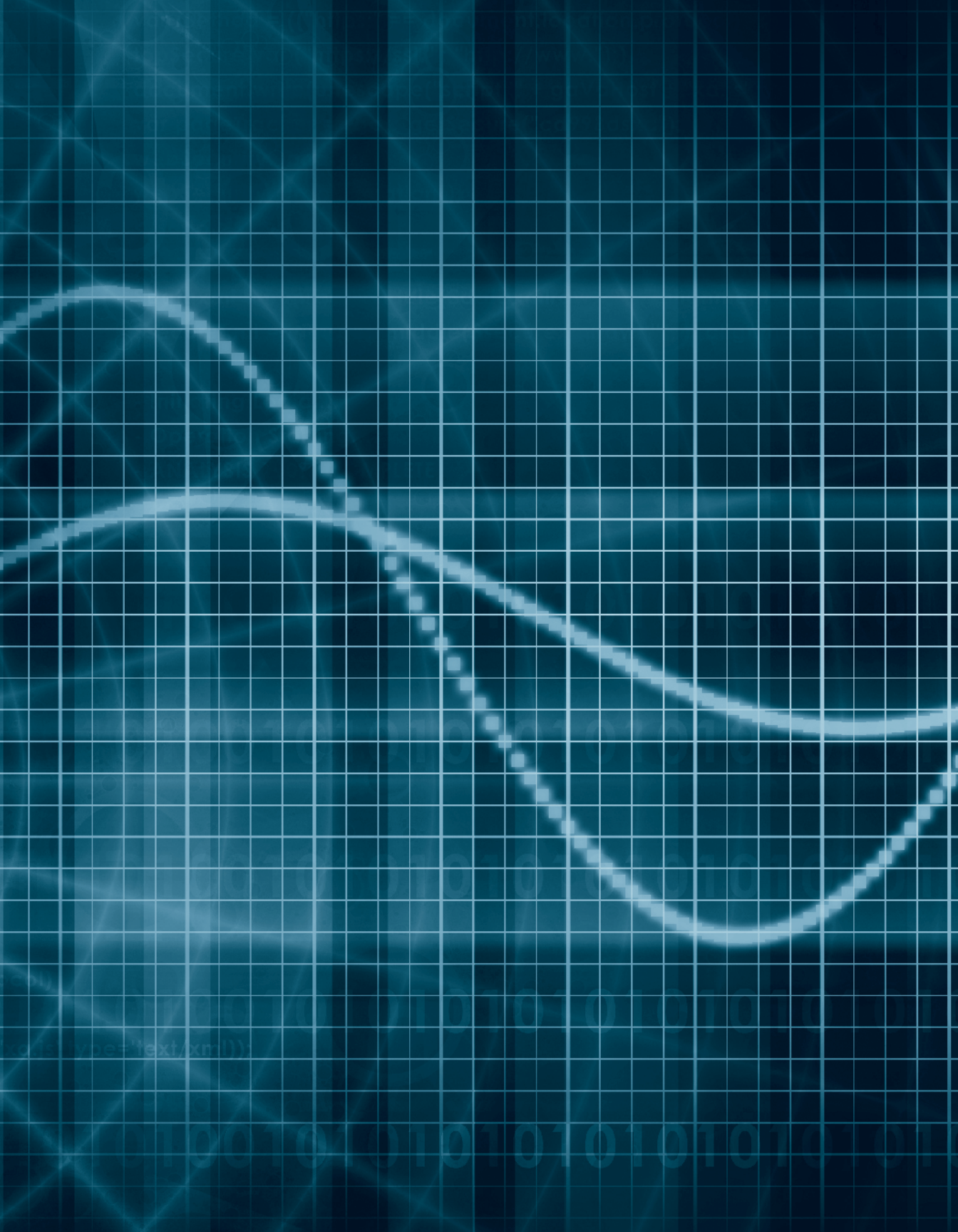
Through wired and wireless networks, carrying voice and data, communications interoperability is built as a complex system of systems. While technology is an inescapable piece of the interoperability puzzle, it alone cannot solve the problem, for it will be forever impossible to build a complete system without human management, operations, and procedural subsystems being integrated far in advance.

SEARCH has been privileged to work with agencies large and small across the country under U.S. Departments of Justice and Homeland Security programs that provide assistance to improve interagency communications among first responders. We've seen great need for resources—human, financial, and technological—to solve this puzzle, but we've also seen growing cooperation among responders from all disciplines and levels of government.

Our intention in creating this *Communications Interoperability Tech Guide* was to share best practices in project planning, procurement, and implementation, as we've come to understand them through agencies making a difference in their own jurisdictions. We're confident that the best practices in this Guide will improve the odds of your project's success.

And, if you need help along the way, we'll be there to support you with technical assistance resources.

Appendix A: Sample Agreements



Appendix A:
Sample Agreements

NORTH CENTRAL TEXAS COUNCIL OF GOVERNMENTS EXAMPLE MEMORANDUM OF UNDERSTANDING

MEMORANDUM OF UNDERSTANDING
INTER-JURISDICTIONAL RADIO MUTUAL AID COMMUNICATIONS
IN THE NCTCOG AREA

(DATE)

We, the undersigned, representing the County of _____, City of _____(the "Agencies") do hereby agree to the following:

Whereas, the Agencies all utilize, and/or plan to utilize, trunked radio systems using technology from a common equipment manufacturer, and/or plan to implement specialized 3rd party equipment designed to provide interoperability between systems from different manufacturers,

Whereas, each of the Agencies desires to improve the quality and timeliness of inter-agency communications during mutual aid operations,

Whereas, each of the Agencies desires to provide other Agencies with direct access to their individual trunked public safety radio system, for the express purpose of cooperation and coordination with neighboring law enforcement agencies,

NOW THEREFORE, The parties hereto jointly agree:

1. Each Agency shall allow the other Agencies to either directly access their respective public safety trunked radio systems, or provide access through 3rd party interoperability equipment.

2. Each Agency shall share with the other agencies all information necessary to configure and program user radios for operation on their respective public safety trunked radio systems.

3. ALL programming information and parameters shall be considered CONFIDENTIAL and shall not be disseminated to any party not included in this Memorandum without the express written permission of the respective Agencies.

4. Direct access is reserved for emergency, priority or other incidents where its use creates a significant advantage to public safety, including felony pursuits, officer needs emergency assistance, lookouts for incidents near political boundaries, perimeter search operations, task force operations, and mutual aid fire scenes. Direct access may also be used to provide communications for pre-arranged activities, such as funeral escorts or parades through two or more jurisdictions.

5. Direct access during "priority" or "emergency" incidents is encouraged. The Agencies are encouraged to develop guidelines that permit field users to directly access neighboring trunked systems in a timely manner by notifying their dispatcher prior to switching. Telephone coordination between dispatch centers is not necessary.

6. In cases where two Agencies share a common border, it is recommended that the Agencies share the appropriate "dispatch" and "primary tactical" talkgroup used in the adjacent jurisdictions and/or "districts", "patrol areas" or "beats".

7. Plain English shall be used for all mutual aid communications. "10codes", "signals", jargon, and slang phrases shall not be used.

8. Field units shall identify themselves by stating their agency name and unit designator.
   Examples:
   "DFW Airport Unit 131"
   "Arlington Unit Three Forty Four"
   "Fort Worth Three Adam Eighty One"
   "Grand Prairie Unit 367"
   "Collin County Unit Three Ten Baker"
   "Grapevine Baker 211"
   "Carrollton Unit One Twenty Four"

9. When communicating with field units from neighboring jurisdictions, dispatch center personnel shall identify themselves by stating their agency name.

10. In the case of "short term", "priority", "emergency", and "notification" communications, once the need to communicate directly with a neighboring jurisdiction has been established, the field user shall inform their home dispatcher of their intention to switch, and only make the switch after dispatcher acknowledgement and clearance. If possible, the field user shall leave a radio on their home channel, in case their dispatcher or other units need to establish contact with them.

11. When calling a neighboring jurisdiction, the field user shall state their unit identification as described above, the word "to", and the name of the agency that they are calling. The field user shall then wait for the dispatcher to respond before giving any additional information. Example:

    "Arlington Three Adam Eighty One to City of Ft. Worth."

12. Provided that the channel is not currently in use, the neighboring jurisdiction's dispatcher should respond immediately. If the channel is in use, the dispatcher will ask that the calling user stand by. Example:

    "City of Ft. Worth to Arlington Three Adam Eighty One, go ahead."

13. After their call is acknowledged, the calling user shall state the reason that they are calling and what, if any action the neighboring agency needs to take. Example:

    "We have a bank robbery that just occurred in Arlington on I-20 just east of the city line. The direction of travel was westbound on I-20 into Ft. Worth. I have lookout information when you are ready to copy."

    "I am on the scene of an accident with injury that just occurred on I-30, just west of border between Arlington and Ft. Worth. I need one of your units to respond to this location, and start rescue for one patient with minor injuries."

14. Once initial contact has been established and the reason given for the call, the communication shall proceed in a normal fashion until complete. Before returning to their home radio system and channel, the calling user shall state their unit designator and inform the neighbor dispatcher that they are switching back to their normal channel. Example:

    "Arlington Three Adam Eighty One, I have no further traffic. I am switching back to Arlington PD Channel 1."

15. In the case of "long term" and "static" events where mutual aid assistance is requested by an Agency of another Agency, a supervisor shall contact the neighboring Agency or cause the neighboring Agency to be contacted, and a formal request shall be made for mutual aid assistance in accordance with existing mutual aid agreements. If approved, the assisting Agency shall be provided with the specific type of assistance required (K-9, helicopter, ambulance, etc.) by the requesting Agency. The assisting Agency shall be provided with the talkgroup or channel where communications for the mutual aid operation are being conducted by the requesting Agency. The assisting agency shall determine appropriate unit(s) to respond to the mutual aid event, and provide the above information to the responding unit(s) at time of dispatch. Once all information is received, the responding unit(s) shall switch to the designated talkgroup on the requesting Agency's trunked radio system and initiate contact as outlined in Paragraphs 10-13 above.

16. Complaints of abuse or unauthorized operation by users from neighboring jurisdictions are encouraged to be resolved at the field supervisor level as soon as possible after an alleged problem occurs. If the complaint cannot be resolved at this level or if the severity warrants, a complaint in writing can be made to the jurisdiction involved. Written complaints shall include the date and time of the offense, the nature of the complaint, the six-digit radio identification number, the name of the person who witnessed the offense, and, if available, any audio recording of the offense. Complaints of abuse or unauthorized operation shall be resolved using established internal procedures, and a written response detailing the action taken shall be sent to the complaining Agency within 30 working days of the initial complaint.

17. New law enforcement or Fire/EMS agencies may be added by amendment to this Memorandum from time to time, subject to the approval of the Agencies.

18. Nothing in this Memorandum shall be construed as to prohibit any individual Agency from entering into mutual aid communications agreements with separate law enforcement or fire/EMS entities not included in this Memorandum. Under no circumstances shall any Agency disseminate another Agency's programming parameters to any third party without express written approval from the other Agency.

19. Each Agency shall assume full responsibility for all costs associated with programming their radios for direct access.

20. During times of law enforcement or fire mutual aid operation, each Agency shall make every reasonable effort to provide the same level of communications support to units from neighboring Agencies as they would to their own units.

21. Each Agency shall designate a representative to serve on a NCTCOG Mutual Aid Communications Committee. On an annual basis, the chair of this committee will be rotated through all member agencies, by alphabetical order. These representatives shall meet on a quarterly basis, or more frequently as required, to identify and resolve any issues that arise during mutual aid or direct access. In the event that an Agency's representative is no longer available due to reassignment, the Agency shall appoint a new representative and inform the committee Chairperson in writing.

LOS ANGELES REGIONAL TACTICAL COMMUNICATIONS SYSTEM MEMORANDUM OF UNDERSTANDING

LOS ANGELES REGIONAL
TACTICAL COMMUNICATION SYSTEM
MEMORANDUM OF UNDERSTANDING BETWEEN
PARTICIPATING LOCAL, STATE, FEDERAL, AND MILITARY
AGENCIES, FOR RADIO COMMUNICATIONS

This Memorandum of Understanding (MOU) between participating Local, State, Federal, and Military agencies, and the Los Angeles Regional Tactical Communications System Executive Committee, establishes policy and procedures for the activation, use, and deactivation of an interoperability communication system. This system will be known as the Regional Tactical Communications System (*LARTCS*).

PURPOSE

The purpose of the *LARTCS* is to allow direct voice communication between participating agencies in dealing with both short term (felony pursuits, fires, hazmat, etc.) and long term incidents (major disaster, large scale fires and floods, civil disturbances, terrorist incidents, etc.). The *LARTCS* cross-connects different radio channels over various radio frequency bands, throughout the Los Angeles region. This will enhance the safety of participating agencies through real time, field unit-to-unit, direct voice communication interoperability.

SCOPE

A "participating agency" shall be defined as any local, state, federal, or military agency that has read, agreed, signed, and will abide by this MOU.

POLICY

A. Any supervisor of a participating agency may request the activation of the *LARTCS*. These personnel shall be held accountable for radio discipline by their respective agencies.

B. Each communications center will assign the appropriate access channel for their agency that will be linked to the *LARTCS*. For agencies participating in specific incidents, each affected communications center shall monitor the *LARTCS* to ensure requested resources are provided, as well as compliance with this agreement and other policies.

C. During an incident, any agency communication center, incident commander, or supervisor may deactivate use of the *LARTCS*, based on operational needs. Notice to other agencies on the *LARTCS* will be given when use is deactivated.

D. Deactivation of the *LARTCS* shall be a joint decision by the involved agencies.

E. All personnel broadcasting on the *LARTCS* will use **plain spoken English**. The use of radio codes, acronyms, and abbreviations, are to be avoided as they have different meanings for different agencies. Due to agency terminology differences in use of plain text of words such as "Help", "Assistance", "Repeat", and "Back-up", the use of these words shall be followed with a brief description of why the above is needed. (i.e., officer requesting assistance with traffic control, etc.). The use of the word "Help" should be avoided unless it is being used in the universal context in a life-threatening incident.

F. Due to the fact the various radio frequencies used in the systemmay be monitored by the general public, **only non-classified information may be passed over the *LARTCS***. Any confidential or classified communications shall be made through other secure means.

G. The *LARTCS* may be activated or used for emergency joint agency incidents. However, it may also be used for planned joint agency tactical operations, large public events, joint training exercises, and planned system testing. The type and priority of incidents are as follows:

Priority 1: Disaster and extreme emergency operations.

Priority 2: Emergency or urgent operations involving imminent danger to the safety or life and property.

Priority 3: Special event control activities, generally of a pre-planned nature, and generally involving joint participation of two or more agencies.

Priority 3a: Drills, tests, and exercises.

These priorities conform to the State Office of Emergency Services (OES) CLEMARS mutual aid plan. Priority 4 level communications (single agency secondary communications) are not covered by this MOU, and are not to be used on the *LARTCS*.

H. A request to participate in the *LARTCS* is not a request to transfer responsibility of an incident.

I. The *LARTCS* could be used for Homeland Security or other related incidents. It shall be the policy of the *LARTCS* for the participants not to release the radio frequencies, CTCSS/CDCSS codes, channel plan, and other information related to the system. No system information shall be released to the media or other entities, public or private. Exception: anyone involved with the direct maintenance or repair of the participating agency's radio equipment. This information shall be provided to service technicians on a "need to know" basis only. Failure to safeguard the *LARTCS* information may be cause for suspension or cancellation of this MOU with the offending agency.

PROCEDURES

As previously stated in this document, the *LARTCS* is intended for use when immediate information will enhance the safety or effectiveness of personnel dealing with an incident. It is not to be used to deliver mundane information. The *LARTCS* may be requested, if needed, to allow voice communications between each agency's command personnel dealing with the incident. Specific procedures will be defined in the *LARTCS* Operations Manual.

MAINTENANCE

Each participating agency is responsible for the maintenance of the involved hardware and software for their agency. All participating agencies shall be responsible for their own connection maintenance costs, if any. The Los Angeles County Sheriff's Communications Bureau shall maintain the infrastructure of the *LARTCS*.

It is understood that radio reprogramming and maintenance will be required on an ongoing basis, and system configuration changes will occur as the system grows. Participating agencies agree to promptly reprogram their radio equipment as necessary, in order to maintain continuity of the system.

For uniformity of identification in radio displays, radio frequencies in each band will be labeled as specified in the *LARTCS* Operations Manual.

CONTROL

A. There is an Executive Committee representing all participating agencies.

B. The Commander of the Los Angeles County Sheriff's Department, Communications and Fleet Management Bureau, will assume the duties of System Coordinator for the *LARTCS*. The System Coordinator will coordinate and maintain copies of original Memorandums of Understanding for this system and the associated communications agreements for the *LARTCS*. The System Coordinator can be reached at Communications and Fleet Management Bureau, 1277 North Eastern Avenue, Los Angeles 90063. (323) 267-2501.

C. The System Coordinator will forward any complaints, concerns, or proposed changes to the Executive Committee, for review and appropriate action.

AGREEMENT OF PUBLIC SAFETY AGENCY

Any Local, State, Federal, or Military agency may participate in the *LARTCS* by signature of agreement by the department head or their designee, on this MOU. The System Coordinator will notify all other participating agencies of any new member agencies.

REVISIONS

This MOU may be revised or amended at any time by mutual agreement of participating agencies. Any participating agency may terminate their participation by giving written notice to the System Coordinator. The System Coordinator will notify all other participating agencies of the withdrawal.

The _____agrees to this Memorandum
AGENCY

Of Understanding, and will conform to its policies and procedures.

DEPARTMENT HEAD SIGNATURE	TITLE	DATE
PRINT DEPARTMENT HEAD NAME		
DESIGNEE SIGNATURE		
PRINT DESIGNEE NAME		
AGENCY ADDRESS	TELEPHONE	
AGENCY 24 hour contact (duty agent/response/dispatch)	TELEPHONE	E-MAIL ADDRESS
AGENCY 24 hour technical contact	TELEPHONE	E-MAIL ADDRESS

NEW ORLEANS
MARITIME INTERCOMMUNICATIONS COMMITTEE
OPERATIONAL GUIDELINES

Operational Guidelines

Rev. 8/24/03

NEW ORLEANS MARITIME INTERCOMMUNICATIONS COMMITTEE (NOMIC)

Definition

The New Orleans Maritime Intercommunications Committee (NOMIC) is a collaboration of local, state and federal agencies working in concert to build a seamless interoperability communications network linking port control and first response agencies.

Purpose

The purpose of this committee is to:

- Provide rapid and reliable means by which to exercise command, control and coordination of mobile assets between participating agencies.
- Identify roles and responsibilities of those participating agencies to guarantee continued success of the program within the region.
- Insure participating agencies are aware of the capabilities, limitations and equipment maintenance responsibility of the network.

Controlling authority

a) NOMIC shall act as the sole controlling authority for the program and provide updated information to all agency participants as changes dictate. Furthermore the committee shall coordinate necessary upgrades or repairs with each participating agency.
b) The New Orleans Fire Department communications facility shall house the ACU-1000 audio matrix switch and act as the primary Network Control Station (NECOS) executing requested patches as necessary.
c) Where situations preclude the primary NECOS from performing requested functions, U.S. Coast Guard Group New Orleans shall act as secondary NECOS.

Policy

Interoperability telecommunications patches shall be conducted in accordance with;

- This Operational Guideline
- International Telecommunication Union (ITU) regulations
- Federal Communications Commission (FCC) regulations
- Other instructions and directives issued by proper authority and so distributed by NOMIC.

Operational Guidelines

Inter-operability COMM-SYS

This list illustrates the connectivity of the original Interoperability Communications System.

New Orleans Fire Dept. New Orleans Police Dept. U. S. Coast Guard
New Orleans EMS Jefferson Parish Sheriff Causeway Police
Crescent City Conn. LA. State Police Harbor Police Dept. Fed. Bureau of Invst. U. S. Customs U. S. Border Patrl.
Drug Enforcement Adm.

OTHER SYSTEM PORTS BEING USED
VHS Progr., UHF Progr., 2 Teleco. Circuits, ITAC, ICALL, Remote

Agency responsibility

a) Each participating agency shall be responsible for maintaining equipment provided and attached to the JPS Communications ACU-1000 audio switch.
b) Each participating agency shall provide continual administrative and operational contact information to the NOMIC.
c) Continual operational oversight shall be provided to the NOMIC in an effort to better refine these Operating Guidelines.

Operational Notification

Operational notification to the NOMIC is required for the following situations involving communications equipment.

- ♦ Modifications
- ♦ Removal
- ♦ Installations
- ♦ Changes in capabilities
  - •Changing frequencies
  - •Other modifications which would alter the mode or method on which the equipment was designed to operate.

Communications Equipment Includes (And Not limited To)

- ♦ ACU-1000 Switch or equipment
- ♦ Transmitters
- ♦ Receivers
- ♦ Transceivers
- ♦ Telephones (both land line and cellular)
- ♦ Other telecommunications equipment
- ♦ Antennas and Cables
- ♦ Accessories

Operational Guidelines

Equipment Failure

Any agency detecting equipment failures, whether their own or another agency, must notify the primary and secondary NECOS points of contacts via voice and e-mail at the addresses provided in the POC enclosure to this document.

Step	Action
1	Identify the failure
2	Notify NECOS units
3	Your Agency: Notify your appropriate maintenance entity
	Other Agency: Notify point of contact per POC enclosure
4	Notify NECOS units of repair personnel & arrival time for access and possible estimate time of repair (ETR).

Comms Security (COMSEC)

This interoperability solution is unclassified. Wherever possible, do not divulge information sensitive to any mission.

These circuits offer no communications security. The general public and possible hostile sources will be able to obtain information about multi-agency operations easily by monitor these working frequencies. If joining a patch, any agency may be recorded by another participating agency.

Testing & Training

The NOMIC shall coordinate all testing and training. Individual agency training is encouraged but the NOMIC members should be notified in advance of non-scheduled training between agencies.
Testing and training should be coordinated and scheduled by the NOMIC for all participating agencies.
Testing and training will be scheduled during the last week of each month.

OPERATIONAL COMMUNICATIONS

Guidelines

a) NECOS shall never be requested to coordinate between the requesting and receiving agencies.
b) A single agency's participation on multiple patched circuits can only be accomplished by having more than one radio attached to the ACU-1000 audio matrix switch. Since all participating agencies only have one radio attached, any agency can only participate in one interoperability patch at a time.

Operational Guidelines

Voice Call Signs

Agencies will always identify themselves by agency name and number. Communications personnel shall provide mobile units with appropriate call signs of other government agency units as obtained from other communications watch personnel.

In example: NOPD vehicle 728 has requested communications with FBI 455. NOPD will coordinate through FBI Comm. Center and request NOPD 728 to call "FBI 455" on the designated working frequency.

Example: " NOPD 728 to FBI 455 "

Acronyms & brevity codes

To reduce confusion or misinterpretations between agencies, the use of agency specific acronyms and brevity codes should not be used. Common acronyms are acceptable if it is reasonably sure definitions are universal from agency to agency (i.e. roger for yes or affirmative). Use clear text when possible.

System Purpose

"Official Use Only" Special incidents. Not to be used as a "talk channel".

ACU-1000

The audio switch used to allow interoperability between agencies with disparate radio systems.

Incident Commander

(I/C) The individual directly responsible for command and control of any given incident.

NOMIC Patch:

The joining of one agency's radio system to another agency's radio system, using the ACU-1000.

Requesting Agent

The individual(s) or agency requesting to have their communications channel added to an in-progress incidents communications path.

Request for NOMIC Patch:

This is made by individual or agency wishing to be added into the communications. The request is made to the incident commander.

Authority to Patch:

Authority to add any agency to an existing incident communications is granted to the Incident Commander.

Standard Operating Procedure

Request for Release

Once an agent or agency has been relieved and no longer wishes to be part of the Incident Communications Path, the agent or agency will notify NECOS to remove his/her agency from the patch.

Contact Person to Initiate a Patch:

The I/C shall contact the NECOS to authorize NOMIC patches. The I/C has the authority to request that any agency be removed from a particular Incident Communications Path.

Authority of an Incident

The I/C is the individual directly responsible for command and control of any given incident. The I/C will authorize any interoperability patches as needed to effectively command and control a given incident.

Authority to add Agency to Patch

The authority to add any agency to an existing incident communications is granted to the I/C or his designee.

Request for Inclusion into a Patch

The agency requesting to be patched into an ongoing incident should contact the I/C for authorization. The I/C should be contacted by contacting the I/C's communications center. The I/C should send his request through his communications center. The requesting agency shall notify their dispatch of the intended patch and obtain clearance from their agency for the patch.

Contact Point for NECOS

The contact point to establish patches within the New Orleans area is NECOS. **REFER TO POC DOCUMENT FOR NAMES AND NUMBERS** A log will be kept, with the following: Date, Time, and Agencies on a given patch, and I/C's name and agency.

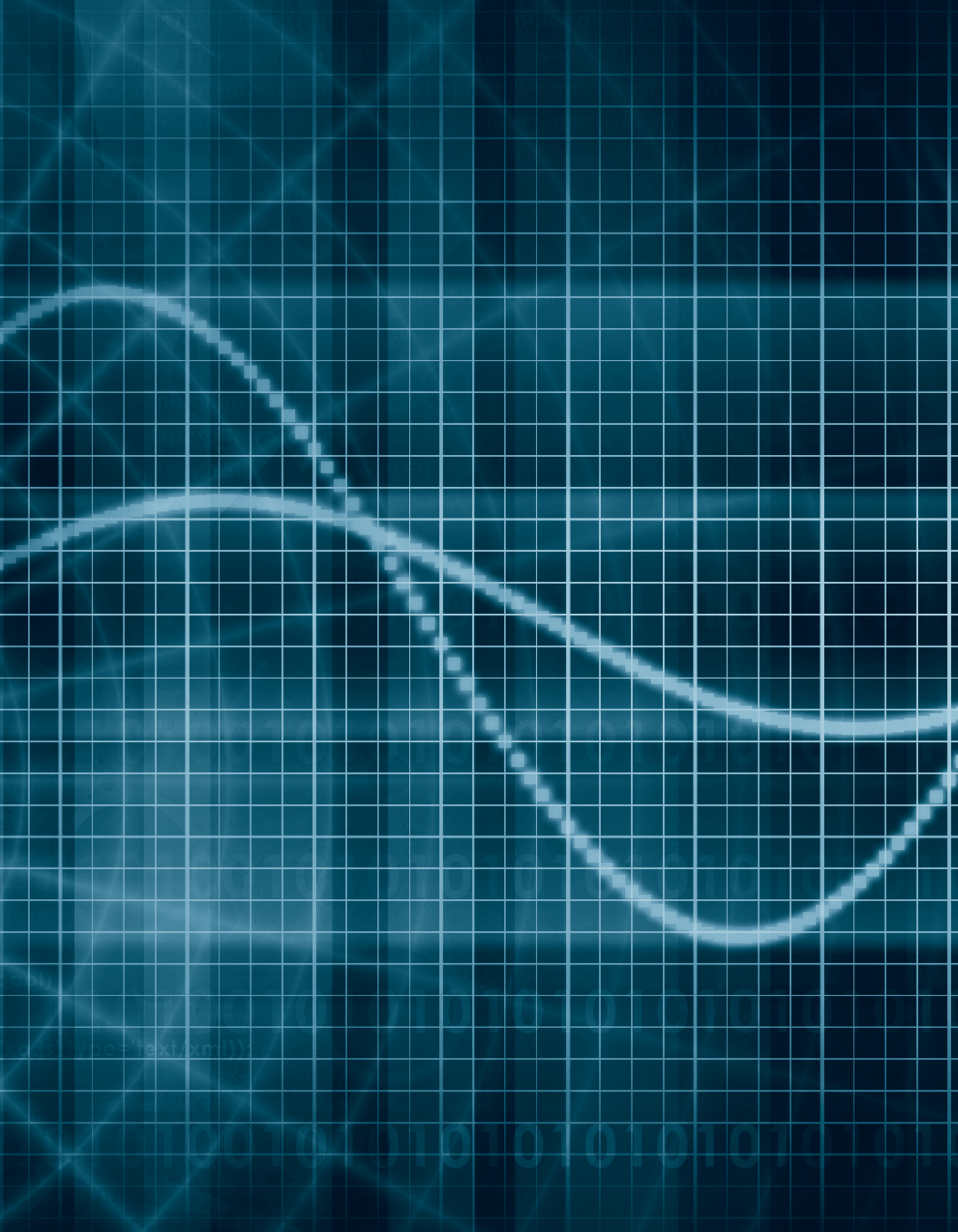
Release from a NOMIC Patch

The agency requiring release from the NOMIC patch should contact the NECOS upon conclusion of that agency's participation in the incident. The I/C may elect to disengage any agency he deems appropriate during the incident. NECOS will log who requested the release and the date and time of the release. Any agency participating in a patch may choose at any time to stop participating in a patch without any additional authority. If a participating agency wants to be released from a patch, the agency should notify the I/C.

Pre-planning of likely Incidents

Any agency participating in the MOU can request a pre-plan of a likely incident. This agency should identify who the agency would like to be able to communicate with during a given incident and those patches can be preset. The preplanned patches would then be authorized by the I/C of an incident. Each agency in the preplan would authorize his agency's participation.

Appendix B:
SOP Example



Appendix B:

SOP Example

Courtesy of the Metropolitan Emergency Services Board, St. Paul, Minnesota.
www.metro9-1-1board-mn.org

INTERIM **INTERIM**

800 MHz Trunked Regional Public Safety Radio System
Standards, Protocols, Procedures

Document Section:	**3 - Interoperability Guidelines**	TOC Recommended
Sub-Section:	**3.1f**	
Procedure Title:	**Use of Regional 800 MHz to Metro Emergency Interoperability**	Date: 5/24/01
Date Established:	**2/12/01**	
Replaces Document Dated:	**5/14/01**	MESB Approval
Date Revised:	**5/30/03**	Date: 06/06/03

1. Purpose or Objective:
Establish procedures for use of patched regional 800 MHz to Metro Emergency UHF (MET-EMRG-UHF) channel interoperability radio facilities for interagency communications when coordination is required between law enforcement users of UHF radio systems and law enforcement users of the regional 800 MHz trunked radio system.

2. Technical Background:

- **Capabilities**

A UHF radio system covering the City of St. Paul, the University of Minnesota and Minneapolis-St. Paul International Airport is available for use by personnel of government entities using UHF radio systems that need interagency communications to coordinate activity with personnel of entities that use the new regional 800 MHz trunked radio system. This UHF interoperability radio system includes an UHF infrastructure on the State of Minnesota Metro Emergency UHF radio channel that can be hard patched to a regional 800 MHz trunked radio system talk group.

- **Constraints**

One regional 800 MHz talk group can only be in one patch.

3. Operational Context:
The patch between the Metro Emergency UHF channel and the corresponding regional 800 MHz radio system talk group should only be used when there is a significant need for communications to support coordinated activities between personnel of entities that are on UHF radio systems and personnel of entities that are users of the regional 800 MHz radio system.

The Metro Emergency channel and the associated patched regional 800 MHz talk group may be used for short-term high intensity events, and for long-term extraordinary events.

INTERIM **INTERIM**

The Metro Emergency UHF channel patched to a regional 800 MHz talk group should be used only if other suitable means for interagency communicating are unavailable or if the other available means for coordination communications are insufficient for the needs. Other means may include use of radio to radio cross band repeaters (*See Interoperability Guidelines Subsection 3.3c*) between tactical channels at the scene, and radio console soft patching of a preauthorized agency UHF tactical channel to a RF control station on a talk group on the regional 800 MHz radio system (*See Interoperability Guidelines Subsection 3.3b*).

4. Recommended Protocol/ Standard:

It is recommended that there be a regional 800 MHz pool talk group, METEMERG, hard patched to the Metro Emergency UHF channel.

The regional 800 MHz METEMERG talk group shall not be part of any multi-group.

No personnel in any dispatch center shall soft patch the UHF metro emergency channel to a RF control station on a regional 800 MHz trunked talk group (*See Section 3.3b RF Control Stations and Portables*).

It is recommended that the regional 800 MHz METEMERG talk group be included in scan lists of all law enforcement radios on the regional 800 MHz radio system.

The METEMERG talk group on the regional 800 MHz radio system shall be recorded *(See Section 3.1h).*

TG Requirements	For Whom?
Highly Recommended	None
Recommended	Metro Law Enforcement
Optional	None
Not Allowed	None

Cross Patch Standard	YES/NO	To Talk Group(s)
Soft Patch	No	NA
Hard Patch	Yes	MET-EMRG-UHF

5. Recommended Procedure:

Most of the time, an event that requires interagency coordination will begin on a main dispatch radio channel of one of the public safety dispatch centers. When it becomes apparent that interagency coordination of law enforcement agencies will be needed (and possibly fire and EMS), and coordinating participants are on UHF and on the regional 800 MHz systems, a dispatch center operator should advise the UHF radio users to switch to the Metro Emergency UHF channel.

INTERIM **INTERIM**

Dispatch center operator support, and the decision to use the Metro Emergency UHF channel patch to the METEMERG talk group, shall be performed by a dispatch center operator in the center responsible for the agency that started the event.

6. Management:

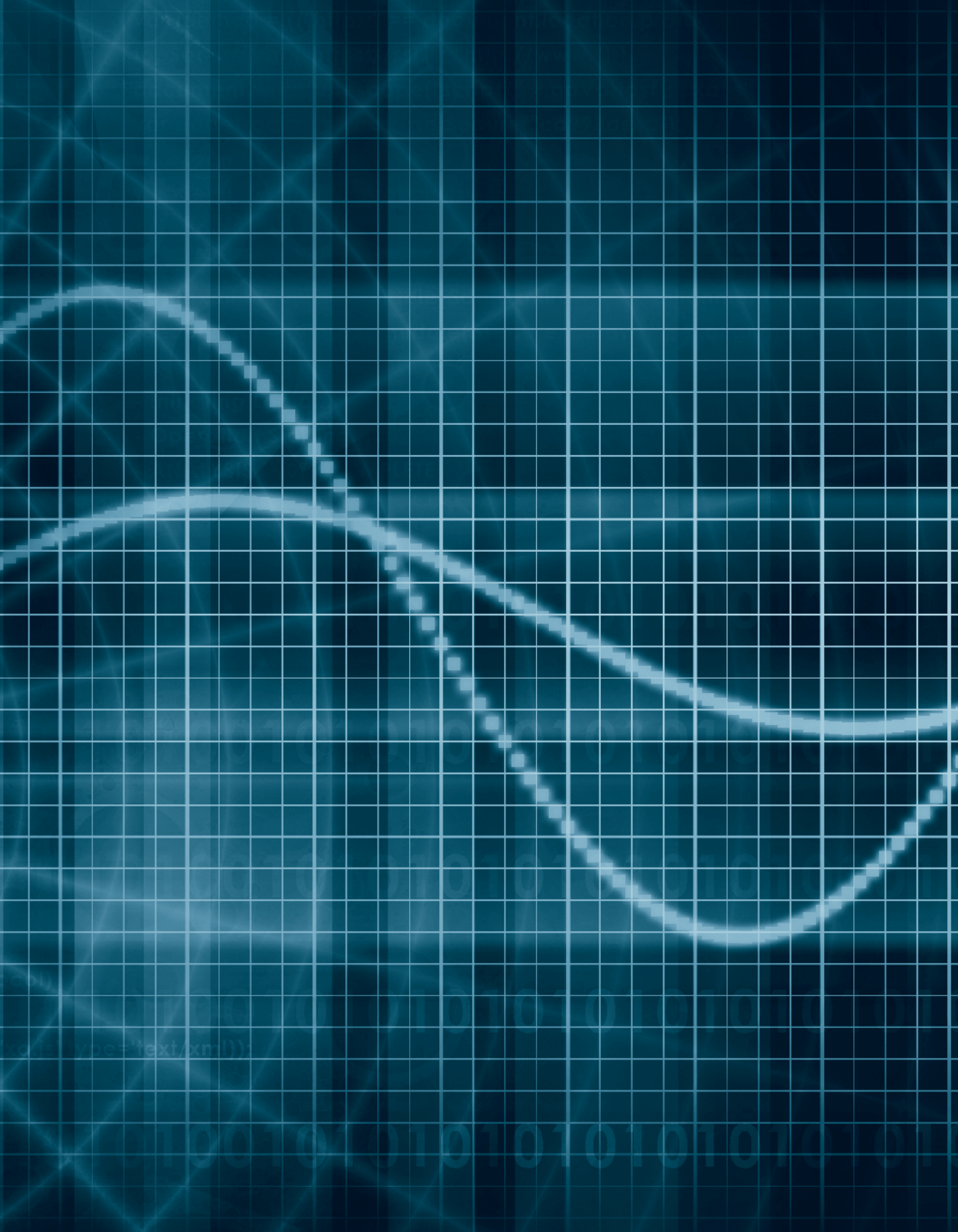
The dispatch center managers for agencies on the regional 800 MHz radio system shall insure that there is a procedure for use of the Metro Emergency UHF channel to METEMERG talk group patch in the dispatch center for which they are responsible.

Dispatch center operators shall receive initial and continuing training on the use of this procedure.

Responsibility for monitoring performance and for modifying this procedure shall be a function of the Technical Operations Committee of the Metropolitan Emergency Services Board.

The development of and the management of statewide rules for use of the Metro Emergency UHF radio channel shall continue to be the responsibility of the Metro Emergency Channel Users Committee. All users of the Metro Emergency Channel and the regional 800 MHz radio system METEMERG talk group shall comply with the Metro Emergency Channel operation rules; and with the MINSEF rules when the Metro Emergency channel is patched to the MINSEF VHF frequency.

Appendix C:
ICS Communications Position Duties



Appendix C:
ICS Communications Position Duties

Position task books serve to prepare individuals for roles during response and also define responsibilities applicable to Incident Command System (ICS)-oriented response more generally. The National Wildfire Coordinating Group (NWCG) created task books formalizing responsibilities of ICS positions for wildfire response. The NWCG task books provide the most comprehensive list of duties available at this time for describing the Incident Communications Center Manager (INCM) and Radio Operator (RADO) responsibilities. The DHS Office of Emergency Communications (OEC) modified the NWCG task books for use in the All-Hazards Communications Unit Leader (COML) and Communications Technician (COMT) programs. Included below are responsibilities specific to these communications functions.[1]

Communications Unit Leader (COML)

Competency 1: General

1. Obtain and assemble information and materials needed for a response kit prior to receiving an assignment, including critical items needed for the assignment and items needed for functioning during the first 48 hours. The following items are suggested as basic information and materials kept in a go bag:

Reference Materials

- Appropriate ICS forms and logs
- Current Tactical Interoperable Communications Plan (TICP) and Statewide Communications Interoperability Plan (SCIP), if available
- Inventories or other lists of local and regional communications response equipment
- Preplanned local system coverage maps
- Contact, capability, and availability information for local and regional Communications Technicians and Specialists
- Field Operation Guide (NIFOG)
- COML Mobilization Guide (specific to locality)

1. The following has been adapted from current editions of both the NWCG and the OEC task books. The NWCG task books are available at www.nwcg.gov/pms/taskbook/logistics/logistic.htm. OEC task books are available through the Statewide Interoperability Coordinators.

Supplies

- Pads of paper, pencils, pens, and tape
- Portable radio(s) as appropriate for the region
- Personal items (including medicine and cash), food and beverage to be self-sustained for 48 hours or more
- Radio programming equipment (cloning cable or computer), adapters, and suitable tools
- GPS
- First-aid kit
- 24-hour clock
- Multi-purpose knife

2. Establish and maintain positive interpersonal and interagency working relationships.
   - Through briefings, discuss EEO, civil rights, sexual discrimination, and other sensitive issues, with assigned personnel
   - Create a work environment that provides diversity and equal opportunity for all personnel assigned to the incident
   - Provide equal assignment opportunities based on individual skill level
   - Monitor and evaluate progress based on expected work standards
3. Provide for the safety and welfare of assigned personnel during the entire period of supervision.
   - Recognize potentially hazardous situations
   - Inform subordinates of hazards
   - Provide safety and identifying equipment, such as vests identifying the communication's function, flashlights, and glow sticks
   - Ensure that special precautions are taken when extraordinary hazards exist
   - Ensure adequate rest, hydration, and nutrition is provided to all unit personnel
   - Recognize any special medical needs of all unit personnel

Competency 2: Mobilization

4. Obtain complete information from the public safety communications center(s) serving the area and incident upon initial activation, including:
   - Incident name and, as appropriate, an order, request, or other unique number identifying the incident for tracking purposes
   - Reporting location
   - Reporting time
   - Transportation arrangements/travel routes
   - Contact procedures during travel (telephone/radio)
5. Gather information to assess the incident assignment. This is an ongoing task throughout all phases of the incident. Include assigned resources in a draft Incident Radio Communications Plan (ICS Form 205). Examples of important information include:
   - Frequencies and/or talkgroups already assigned
   - Other mutual aid channels or equipment already in use
   - Gateway or other interoperability devices already in use
   - Other current incidents or events that may create conflicts with communications plans or tax resources
6. Contact Local Communications Coordinator or Communications Duty Officer (CDO) at NIFC or any local or state resources as necessary to determine frequencies and equipment assigned to the incident (if appropriate for this incident).
7. Arrive at incident and check in. Arrive properly equipped at the assigned incident location within acceptable time limits.
8. Obtain briefing from supervisor. Examples of briefing items are:
   - Work space
   - Work schedule
   - Policies and operating procedures
   - Current resource commitments and expectations
   - Current situation
   - Expected duration of assignment
   - Special needs

This list is not all inclusive; COML is responsible for asking adequate questions.

9. Receive Incident Action Plan (IAP) or Incident Briefing Form (ICS Form 201), if developed. Determine support needs to meet the IAP.
10. Determine requirements for communications to be established and place the initial order. Using information obtained from IAP, section briefings, and agency briefings, immediately order (using proper procedures) supplies, materials, and equipment necessary to support projected incident size.
11. Evaluate needs and order supplies, materials, and personnel to keep unit operating.
    - Order materials and supplies using procedures established by the section chief
    - Maintain quantities of supplies and materials at a level to prevent shortage of any basic needed items
    - Ensure adequate personnel to support the communications unit, technicians, radio operators, etc.
    - Coordinate with the participating agencies for any or additional interoperability resources that may be needed
    - Assess current tactical communications equipment needs such as power sources for extended operations
12. Organize and supervise unit.
    - Brief and keep subordinates informed and updated
    - Establish unit time frames and schedules
    - Assign and monitor work assignments
    - Review and approve time
    - Develop team work
    - Provide counseling and discipline as needed
    - Follow established procedures for reporting inappropriate actions involving contractors, military, or other personnel
    - Brief relief personnel
13. Participate in incident planning meetings as the technical expert for communications needs.
    - Determine the feasibility of providing the required communications support
    - Provide operational and technical information on communications equipment available for the incident

- Provide operational and technical information on communications equipment and systems capabilities and restrictions
- Coordinate with other Communications Unit Leaders under any Area Command established to share information and assure communications interoperability

14. Design communications systems to meet incident operational needs.
    - Determine additional resource needs and order necessary equipment and personnel
    - Prepare Incident Radio Communications Plan (ICS Form 205)
    - Request any additional communications vendor services (e.g., telephone, SATCOM, or microwave) and identify costs associated with equipment
    - Coordinate, through the chain of command, the locations for equipment to be installed (e.g., repeaters, satellite telephones, or telephone lines)
    - Provide communications support for external and internal data operations.
    - Order frequencies following the proper procedures
    - Create diagrams of current communication system(s)
    - Determine optimal locations for any future expansion of communications equipment using topographical maps to evaluate elevation and separation needs
15. Install communications equipment.
    - Obtain equipment from supply unit, if one exists and/or from authorized sources
    - Provide for the installation of and test all components of the communications equipment to ensure the incident's systems are operational, for example:
        - Command repeater
        - Logistics repeater
        - Links (radio and wire-based)
        - Remotes
        - Gateways
        - Aircraft and other special needs
    - Develop installation priorities, while adhering to safety standards regarding communications needs of tactical personnel (i.e., operations before logistics)
    - Clone or program radios as necessary and authorized

16. Assign communications equipment.
    - Identify kinds and numbers of communications equipment to be distributed to specific units according to the communications plan
    - Provide resources and unit leaders with appropriate equipment based on the communications plan
    - Provide basic training as needed on equipment being fielded
    - Maintain equipment inventory to provide accountability
17. Establish Incident Communications Center (ICC).
    - Coordinate location of ICC with Facilities Unit Leader
    - Locate ICC close to the incident command post and away from high traffic areas and noise
    - Locate ICC away from radio frequency and electronic noise
    - Verify Estimated Time of Arrival (ETA) of communications personnel and establish assignments based on incident requirements. Set schedules around operations requirements
    - Obtain necessary supplies for ICC to function properly
18. Manage operations of the ICC.
    - Document radio/telephone activities on appropriate forms
    - Set up filing system for ICC documentation
    - Direct radio/telephone traffic to proper destinations
    - Establish notification procedures for emergency messages
    - Identify system problems, both technical and operational, and determine appropriate solutions
    - Follow established routing procedures for messages
19. Coordinate frequencies, activities, and resources with communications resource coordinators outside of the incident.
    - Contact communications coordinators and notify them of incident frequency, talkgroup, mutual aid channel, dispatch center, or other shared resource assignments, as appropriate
    - Identify communications equipment and personnel that are excess to incident needs and demobilize if appropriate
    - Identify resources as to type/qualifications, quantity, and location
    - Provide a copy of the ICS Form 205 to other agencies or to the COML at any nearby incidents as necessary to avoid interference or other conflicts

20. Notify appropriate local, county, regional, State and/or Federal agencies on adjacent incident(s) of system design and frequency allocations.
21. Initiate and maintain accurate records of all communications equipment.
    - Initiate and maintain accountability system for issuing hand-held radio resources
    - Document geographic locations of equipment and transfer this information to local maps (latitude/longitude, legal)
    - Keep records for local and national resources to ensure return to proper locations
22. Perform operational tests of communications systems throughout the duration of the incident.
    - Identify and take necessary action to accomplish minor field repair or place orders for replacement of equipment
    - Monitor all gateways in use
    - Plan for battery replacement
    - Act decisively to minimize interruptions in system operation
23. Interact and coordinate with appropriate unit leaders and operations personnel.
    - Coordinate with operations regarding system coverage and needs
    - Coordinate with first responders and public safety support organizations regarding needed support (e.g., medical unit for medical evacuation plan)
    - Coordinate with special units (air operations, EOD, SWAT, etc.) for special frequency needs
    - Participate in planning meetings and briefings

Know what other resources may be coming to the incident, such as those from Urban Search and Rescue (USAR), National Interagency Fire Center (NIFC), FEMA, Coast Guard, etc.

24. Identify for release any excess unit resources. Coordinate with unit managers and provide a list of excess personnel and facilities. List will include:
    - Who or what is excess
    - Time and date of excess.

The list will be reviewed daily for accuracy. Follow the established demobilization process, including notification to communications resource coordinators.

25. Maintain Unit Log (ICS Form 214). Unit Log will be kept current, legible, and will document all major activities, which may include:
    - Equipment locations
    - Medical evacuations
    - Personnel changes
26. Evaluate performance of subordinates as required by agency policy and/or permitted by agreement.
    - Discuss performance evaluations with individual(s)
    - Maintain accuracy and fairness
    - List training if needed or desired

Competency 3: Demobilization

27. Demobilization and check out.
    - Submit all required information to the Documentation Unit Leader
    - Receive demobilization instructions from work supervisor
    - Brief subordinate staff on demobilization procedures and responsibilities
    - Ensure that incident and agency demobilization procedures are followed
    - Complete required ICS form(s) and turn in to the appropriate person
    - Ensure that personnel in the unit are demobilized correctly
    - Document lost equipment on agency specific forms

Communications Technician (COMT)

Competency 1: General

1. Obtain and assemble information and materials needed for a response kit prior to receiving an assignment, including critical items needed for the assignment and items needed for functioning during the first 48 hours. The following items are suggested as basic information and materials kept in a go bag:
   - Appropriate ICS forms and logs
   - Tactical Interoperable Communications Plan (TICP), if available
   - Working knowledge of local TICP
   - Inventories or other lists of local and regional communications response equipment
   - Preplanned local system coverage maps
   - Pads of paper, pencils, pens, and tape
   - Food and beverage to be self-sustained for 48 hours or more
   - Portable radio(s) as appropriate for the region
   - Radio programming equipment (cloning cable or computer), adapters, and suitable tools
2. Establish and maintain positive interpersonal and interagency working relationships.
   - Conduct self in a professional manner
   - Respectful and courteous
   - Respectful of public and private property
3. Provide for the safety and welfare of assigned incident personnel during the entire period of supervision.
   - Obtain the safety briefing
   - Recognize potentially hazardous situations
   - Inform subordinates of hazards
   - Provide safety and identifying equipment, such as vests identifying the communications function, flashlights, and glow sticks
   - Provide for security of information
   - Ensure that special precautions are taken when extraordinary hazards exist

Competency 2: Mobilization

4. Obtain complete information from the public safety communications center(s) serving the area and incident upon initial activation, including:
   - Incident name and, as appropriate, an order, request, or other unique number identifying the incident for tracking purposes
   - Reporting location
   - Reporting time
   - Transportation arrangements/travel routes
   - Contact procedures during travel (telephone/radio)
5. Gather information to assess the incident assignment. This is an ongoing task throughout all phases of the incident. Include assigned resources in a draft Incident Radio Communications Plan (ICS Form 205). Examples of important information include:
   - Frequencies and/or talkgroups already assigned
   - Other mutual aid channels or equipment already in use
   - Gateway or other interoperability devices already in use
   - Other current incidents or events that may create conflicts with communications plans or tax resources
6. Arrive at incident and check in. Arrive properly equipped at the assigned incident location within acceptable time limits.
7. Obtain briefing from supervisor. Examples of briefing items are:
   - Work space
   - Work schedule
   - Policies and operating procedures
   - Current resource commitments and expectations
   - Current situation
   - Expected duration of assignment
   - Special needs

   This list is not all inclusive; COMT is responsible for asking adequate questions.
8. Determine requirements for communications as directed by the COML.

9. Evaluate needs and order supplies, materials and personnel to keep/provide necessary communications, as required.
   - Recommend to COML materials and supplies required
   - Monitor levels of supplies and materials at a level to prevent shortage of any basic needed items. Report shortages to the COML
   - Recommend adequate number of personnel to support the communications unit, technicians, technical specialists, etc. to the COML
   - Assess current tactical communications equipment needs such as power sources for extended operations, report findings to the COML
10. Working with the COML, perform as the technical expert for communications needs.
   - Determine the feasibility and required equipment/personnel to provide the required communications support
   - Provide operational and technical information on communications equipment available for the incident
   - Provide operational and technical information on communications equipment and systems capabilities and restrictions
11. Working at the direction of the COML, install or arrange for the installation of communications systems to meet incident operational needs.
   - Through the COML, request any additional communications vendor services (e.g., telephone, SATCOM, or microwave) and help identify costs associated with equipment
   - Through the chain of command, document the locations for equipment to be installed (e.g., repeaters, satellite telephones, or telephone lines)
   - Provide communications support for external and internal data operations
   - Create/update diagrams of current communication system(s)
   - Assist the COML to determine optimal locations for any future expansion of communications equipment using topographical maps to evaluate elevation and separation needs

12. Install, or provide for the installation of, communications equipment.
    - Obtain equipment as needed
    - Install and test all components of the communications equipment to ensure the incident's systems are operational, for example:
        - Repeaters
        - Links (radio and wire-based)
        - Remotes
        - Gateways
        - Telephones
        - Fax
        - Data
        - Aircraft and other special needs
    - In cooperation with the COML develop installation priorities, while adhering to safety standards regarding communications needs of tactical personnel (i.e., operations before logistics)
    - Clone or program radios
13. Assign communications equipment.
    - Provide resources and unit leaders with appropriate equipment based on the communications plan
    - Provide basic training as needed on equipment being fielded
    - Maintain equipment inventory to provide accountability
14. Assist the COML to initiate and maintain accurate records of all communications equipment.
    - Maintain accountability system for issuing hand-held radio resources
    - Document geographic locations of equipment and transfer this information to local maps (latitude/longitude, address, or access instructions)
    - Keep records for local and national resources to ensure return to proper locations

15. Monitor operational performance of communications systems throughout the duration of the incident.
    - Identify and take necessary action to accomplish minor field repair or place orders for replacement of equipment
    - Monitor all gateways in use
    - Plan for battery replacement
    - Plan for generator refueling
    - Act decisively to minimize interruptions in system operation
16. Maintain a Unit Log (ICS Form 214) when required. Unit Log will be kept current, legible, and will document all major activities, which may include:
    - Equipment locations
    - Personnel changes

Competency 3: Demobilization

17. Demobilization and check out.
    - Submit all required information to the COML
    - Receive demobilization instructions from the COML
    - Brief subordinate staff on demobilization procedures and responsibilities
    - Ensure that incident and agency demobilization procedures are followed
    - Complete required ICS form(s) and turn in to the appropriate person
    - Ensure that personnel in the unit are demobilized correctly
    - Document lost equipment on agency specific forms

Incident Communications Center Manager (INCM)

1. Obtain briefing from the Communications Unit Leader (COML).
   - Determine numbers of communications personnel ordered and on site
   - Discuss "check out" procedures for communications equipment; e.g., radios
   - Discuss the specifics of the Communications Plan, ICS Form 205
   - Discuss the current organization of the incident; e.g., section chiefs, unit leaders, and operations staff
   - Discuss how messages from the incident area are handled; e.g., orders from the line or emergency
   - Discuss the Medical Plan, ICS Form 206, and procedures
   - Obtain a copy of the Incident Action Plan and other informational documents from COML; e.g., maps
   - Discuss unit planning meetings and operational period briefings
   - Follow parameters outlined by COML for physical establishment of the Incident Communications Center (ICC)
2. Establish the ICC.
   - Coordinate, with the Facilities Unit Leader, the location of the ICC
   - Ensure the orderly arrangement of supplies and equipment
   - Request sufficient staff to meet the needs of the communications center
   - Order supplies, through the supply unit, to set up and operate the ICC
   - Acquire forms; e.g., ICS Form 210 (Status Change Card), ICS Form 213 (General Message), ICS Form 214 (Unit Log), Telephone Logs, and Radio Logs
3. Assist the COML with the following duties:
   - Maintain equipment accountability and inventories
   - Maintain or, if directed, establish issue accountability system and issue radio resources
   - Maintain or, if directed, establish an inventory accountability system
   - Ensure that issued equipment is operational (includes battery replacement)
   - Tag nonfunctioning equipment upon return
   - Order needed equipment (e.g., batteries), if directed
   - Clone radios
   - Assist user in interpreting the Communications Plan

- Recognize basic communications network malfunctions (e.g., low battery on repeater, intermittent repeater transmissions, or dead spots) and alert COML
- Fill out lost radio reports
- Implement a document filing system
- Ensure information regarding communications restrictions or coverage limitations is disseminated to operations and ICC personnel

4. Supervise and manage the ICC.
   - Carry out established policies, priorities, and operational procedures
   - Provide for safety and general welfare of ICC personnel
   - Directly supervise each Radio Operator (RADO) position; e.g., the use of radio/telephone logs, proper radio procedures, and protocols
   - Brief subordinate(s) and relief personnel. Direct communication is critical. Information is to be given periodically and with every change from planned work
   - Maintain an incident message board
   - Develop and maintain an incident telephone directory
   - Plan and implement an operational period staffing schedule
   - Ensure that proper radio and documentation procedures are followed in the event of an emergency situation

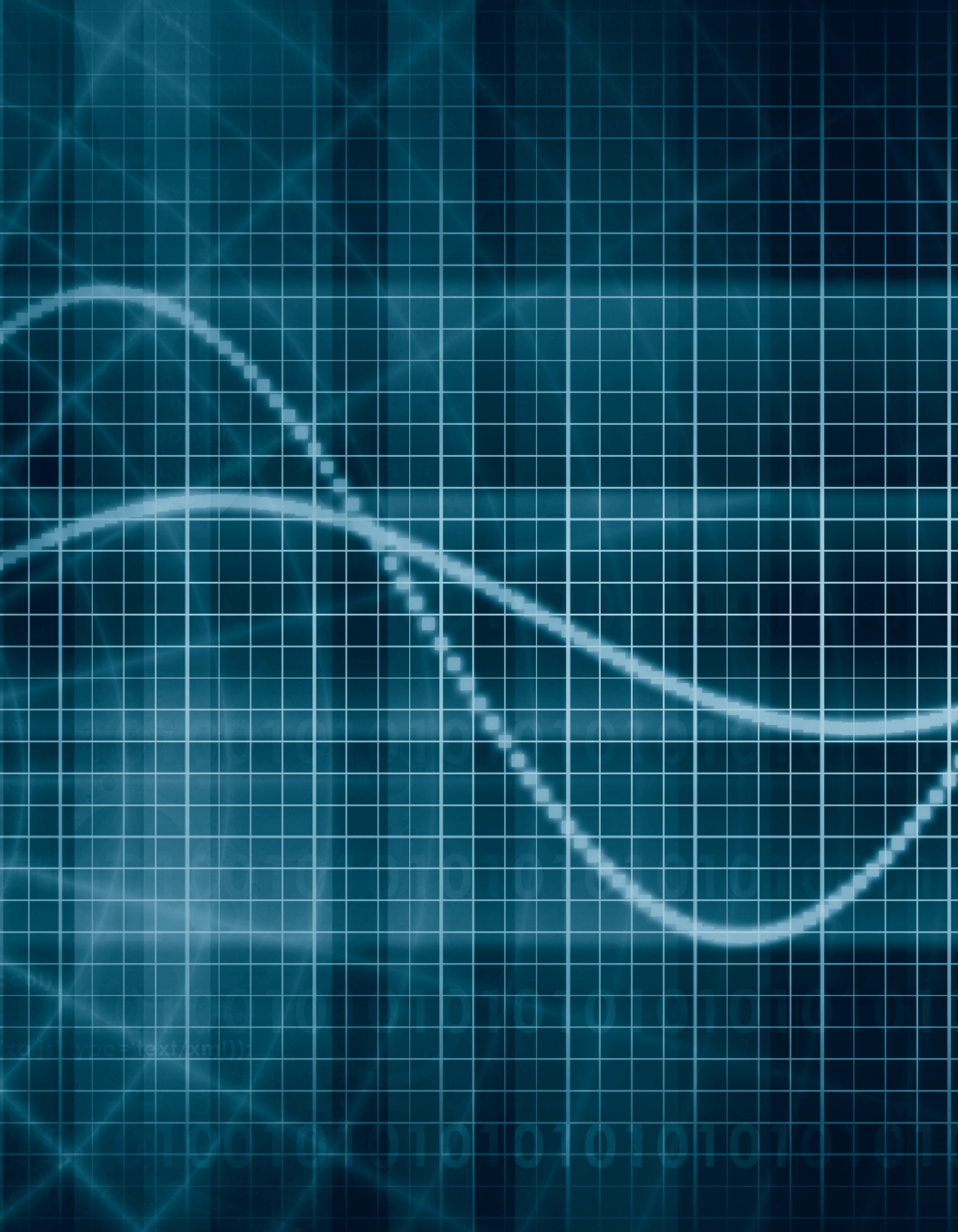
Radio Operator (RADO)

1. Obtain briefing from the Incident Communications Center Manager (INCM).
   - Learn location of units at the incident base camp and Incident Command Post (ICP)
   - Understand time of first work period and discuss work schedule
   - Discuss specifics of the Incident Action Plan (IAP) for the current operational period, particularly ICS 204(s), Assignment List
   - Discuss specifics of the ICS 203, Organization Assignment List
   - Discuss specifics of the ICS 205, Incident Radio Communication Plan
   - Discuss specifics of the ICS 206, Medical Plan and medical evacuation process
   - Discuss allocation of phones to the units and existence of a phone directory
   - Discuss procedure for processing supply orders from the operations area
   - Discuss presence/need for message board

2. Perform duties in accordance with incident communications unit structure.
   - Understand communications unit jobs/positions
   - Understand Incident Command System organizational structure/jobs/positions
3. Perform duties with constructive attitude and skill.
   - Maintain professional demeanor
   - Remain flexible in the face of changing priorities
   - Cooperate with other RADOs
   - Process information as directed
   - Use standard terminology, symbols, designators, and acronyms
   - Continue involvement in decisions
4. Effectively transfer information verbally or in writing.
   - Use correct radio/telephone protocols
   - Communicate with other RADOs and incident personnel
   - Write legibly
5. Participate in communications unit/incident communications center manager meetings.
   - Provide information on radio equipment performance
   - Discuss any information flow problems
6. Demonstrate familiarity with communications equipment, procedures, and basic functions/capabilities.
   - Hand-held, portable, multi-channel radios
   - Radio check-out and check-in procedures
   - Respond with proper frequency when requested
   - Use accountability forms for radio check-out and check-in
   - Procedure for battery check and issuing new batteries
   - Check-out and check-in of appropriate radio accessories
   - Remote phone system (base to line, base to camp, base to helibase)
   - Cellular phone (cell coverage, battery recharging)
   - Facsimile machine
   - Public address system (paging)

7. ICS 213 - General Message.
   - Use the ICS 213 in appropriate situations
   - Correctly demonstrate how to fill out the form
   - Correctly demonstrate how to route the form
   - Complete the follow-up process to close the loop on requests
8. Correctly demonstrate how to fill out and process selected ICS and NFES forms.
   - ICS 210 - Status Change
   - Radio Station Log, NFES 0370
   - Telephone Call Register, NFES 0816
9. Correctly process and file communications paperwork for documentation purposes.
   - Radio logs
   - Telephone logs
   - Incident Action Plans
   - ICS 210 - Status Change
   - ICS 213 - General Message
   - ICS 214 - Unit Log
   - Radio check-out information
   - Other communications-related paperwork
10. Respond with appropriate communications to emergency situations.
   - Medical transport request
   - Medical evacuation request
   - Aircraft emergency
   - Evacuation
   - Search and Rescue
   - Fatality

Appendix D:
Interoperability Self-Assessment Scorecard



Appendix D:
Interoperability Self-Assessment Scorecard

In 2005, the Department of Homeland Security's Project SAFECOM, an electronic government initiative of the President, created a process to assess communications interoperability across agencies and jurisdictions. The following five elements of interoperability and 13 related subelements are used.

Interoperability Continuum Element	Baseline Survey Sub-element
Governance	Leadership Decision-Making Groups Agreements Interoperability Funding Strategic Planning
Standard Operating Procedures	Policy, Practices, and Procedures Command and Control
Technology	Approaches Implementation Maintenance and Support
Training and Exercises	Operator Training Exercises
Usage	Frequency of Use and Familiarity

The process presents one or more questions about the element with sample response statements corresponding to early, moderate, full, and advanced stages of development. It further asks respondents to indicate the stage of development across disciplines, political entities, and levels of government, as appropriate.

In the following pages, a reduced version of the SAFECOM assessment is presented as a self-assessment tool. Its appropriate use is to create a snapshot of capabilities along the 13 subelements. This snapshot is useful for depicting and communicating the level of interoperability across the agency, group, or initiative. Interoperability across disciplines, jurisdictions, and levels of government by each of the subelements is left as a single measure to simplify use of the results.

In completing the assessment, consider all three aspects and answer each question for the predominating influence. For example, if regular, National Incident Management System NIMS-based exercises are planned and conducted with full participation across disciplines, but not between jurisdictions, choose a stage of development best reflecting the impact of that aspect. Use the scorecard below while stepping through each of the subelement descriptions to record choices in one spot.

Chapter 15, **Measuring Interoperability**, provides further suggestions for using the Self-Assessment Scorecard.

		Stage of Development			
Element	**Subelement**	**Early**	**Moderate**	**Full**	**Advanced**
Governance	Leadership				
	Decision-making Groups				
	Agreements				
	Interoperability Funding				
	Strategic Planning				
Standard Operating Procedures	Policy, Practices, and Procedures				
	Command and Control				
Technology	Approaches				
	Implementation				
	Maintenance and Support				
Training and Exercises	Operator Training				
	Exercises				
Usage	Frequency of Use and Familiarity				

Self-Assessment Scorecard

Governance: Leadership

Public Safety Leadership

How would you best describe the fiscal and political support that public safety leaders provide to improve your organization's interoperability?

- The leadership within your public safety organization may understand the importance of interoperability and its role, but has not yet taken any political or fiscal action
- The leadership within your public safety organization has begun to seek political or fiscal support for interoperability
- The leadership within your public safety organization pursues multiple avenues of political and fiscal support for interoperability and makes it an organization priority
- The leadership within your public safety organization has successfully ingrained interoperability as an organizational value such that future leaders are expected to be champions for interoperability support

Political Leadership

How would you best describe the fiscal and political influence that political leaders have on the progress of public safety organizations' interoperability?

- Political leader(s) have not yet provided political or fiscal support for interoperability
- Political leader(s) have begun to provide political support (e.g., attending discussions and/or summits on interoperability, including it on the platform) or fiscal support
- Political leader(s) have demonstrated that interoperability is a political and fiscal priority by taking concrete actions (e.g., establishing funding mechanisms, regional or statewide planning efforts) to improve interoperability
- Political leader(s) act to ensure that interoperability remains a priority across future administrations (e.g., legislation, dedicated appropriations)

Consider the question and how this measure varies across organizations, then choose one of these stages of development.

☐	**Early Development** Government leaders are aware of interoperability needs to support protection of citizens and safety of first responders
☐	**Moderate Development** Government leaders understand the importance of interoperability and provide some political and fiscal support
☐	**Full Development** Government leaders demonstrate that interoperability is a political and fiscal priority and begin to coordinate across jurisdictions
☐	**Advanced Development** Government leaders serve as interoperability advocates and act to ensure long-term political and fiscal support

Governance: Decision-Making Groups

Decision-Making Groups

How would you best describe your organization's involvement in groups of public safety practitioners and leaders that apply operational, technical, and management expertise to remove barriers to interoperability?

- — Your organization may or may not participate in informal interorganization partnership(s) or forum(s)
- — Your organization participates in a mix of informal and formal partnership(s) or forum(s). A formal partnership has a published agreement that designates the group's authority
- — Your organization participates exclusively in formal interoperability planning and governing bodies (e.g., bodies with defined missions, responsibilities, and authorities)
- — Your organization's formal groups proactively recruit new participants, including responders beyond first responders

Does your key interoperability decision-making group:

- — Meet regularly?
- — Have consistent membership?
- — Have governance rules?
- — Disseminate information to all members?
- — Disseminate information to public safety leaders (as appropriate)?
- — Disseminate information to political leaders (as appropriate)?
- — Have the capacity to make recommendations concerning interoperability?
- — Have the capacity to implement its own decisions?

Consider the questions to the left and how this measure varies across organizations, then choose one of these stages of development

☐	**Early Development** No interagency partnerships or forums in place
☐	**Moderate Development** Informal partnerships or forums to address common interests, operations, and technology
☐	**Full Development** Formal interoperability planning and governing bodies with defined missions, responsibilities, and authorities in place
☐	**Advanced Development** Proactive recruiting of new participants to include cross-governmental membership and type of responder

Governance: Agreements

Agreements

How would you best describe the informal practices and formal documentation that establish agreed-upon means to ensure interoperability?

- There may be informal, undocumented agreements that enable interoperability in practice
- Published agreements (e.g., MOU/MOA/MAA, Ordinance, Executive Order, IGA) are enforced with some of the organizations with whom you provide incident response
- Published agreements are enforced with all of the organizations with whom you provide incident response
- There are institutionalized processes to develop and review agreements at least every 3 to 5 years, and after system upgrades and events that test your organization's capabilities

Consider the questions to the left and how this measure varies across organizations, then choose one of these stages of development

☐	**Early Development** Unofficial, informal agreements in practice
☐	**Moderate Development** Some of the necessary agreements (e.g., MOU/MOA/MAA, Ordinance, Executive Order, IGA, and Legislation) in place to address multi-organization communications
☐	**Full Development** All necessary agreements (e.g., MOU/MOA/MAA, Ordinance, Executive Order, IGA, and Legislation) in place to address multi-organization communications
☐	**Advanced Development** Institutionalized processes to develop and review agreements at least every 3-5 years and after significant events and upgrades

Governance: Interoperability Funding

Funding for Capital Investments

How would you best describe how well your funding meets needs for capital investments in interoperability?

- Your organization either does not have funding dedicated to interoperability capital investments (e.g., equipment and other one-time costs), or some funds may be cobbled together
- Your funding does not meet all requirements for interoperability capital investments; difficult allocation decisions may be required
- Your organization has funding for capital investments such that interoperability requirements can be met
- Your organization is working to ensure funding of future interoperability capital investments

Funding for Operating Costs

How would you best describe how well your funding meets needs for operating costs that support interoperability?

- Your organization either has no funding dedicated to operating costs (O&M, leases, staffing), or some funds may be cobbled together
- Your organization has dedicated funding for operating costs in the current budget cycle; source of funding beyond that may be undetermined
- Your organization has dedicated funding beyond the current budget cycle for operating costs
- Your organization is working to ensure funding for interoperability operating costs beyond the time that current sources expire

Consider the questions to the left and how this measure varies across organizations, then choose one of these stages of development

☐	**Early Development** Limited and fragmented funding dedicated to multi-organization communications
☐	**Moderate Development** Long-Term planning begins for partially funded multi-organization communications
☐	**Full Development** Acquisition of long-term funding for multi-organization communications
☐	**Advanced Development** Multiple organizations and standing committees working to strategically acquire and manage sustained interoperability and maintenance funding

Does your organization have joint interoperability funding with other public safety disciplines, political entities, and levels of government?

Governance: Strategic Planning

Strategic Planning

How would you best describe the planning efforts to make decisions, take actions, and create processes that ensure interoperability?

- — No interoperability strategic plan in place; some preliminary planning may have begun
- — Strategic planning process in place and plan under development
- — Strategic plan in place and accepted by all participating organizations
- — Strategic plans reviewed annually and after system upgrades and events that test your organization's capabilities

Consider the questions to the left and how this measure varies across organizations, then choose one of these stages of development

☐	**Early Development** No interoperability strategic plan or strategy in place
☐	**Moderate Development** Strategic planning process in place and plan under development
☐	**Full Development** Formal strategic plan in place and accepted by all participating stakeholders
☐	**Advanced Development** Institutionalized processes to review strategic plans on an annual basis and after significant events or upgrades

Standard Operating Procedures: Policies, Practices, and Procedures

Policies, Practices, and Procedures

How would you best describe the direction provided to first responders to implement interoperable communications?

- Informal policies, practices, and procedures may be in place to address interoperable communications with designated types of responders; none are formal. "Formal" means published and enforced
- Formal polices, practices, and procedures are in place to ensure interoperable communications during planned and day-to-day events (e.g., vehicle pursuit, multiple station response) with designated types of responders
- Formal policies, practices, and procedures are in place to ensure interoperable communications during emergency or out-of-the-ordinary events (e.g., mass casualties, flipped tanker that closed a major highway) with designated types of responders
- Processes exist to develop and annually review policies, practices, and procedures for consistency across designated types of responders

Consider the questions to the left and how this measure varies across organizations, then choose one of these stages of development

☐	**Early Development** Informal policies, practices, or procedures
☐	**Moderate Development** Some formal policies, practices, or procedures
☐	**Full Development** All necessary formal policies, practices, and procedures
☐	**Advanced Development** Processes to develop and regularly review policies, practices, and procedures for consistency across participants

Standard Operating Procedures: Command and Control

Command and Control

How would you best describe the direction provided to first responders to implement interoperable communications?

- Informal command and control SOPs concerning interoperability may be in place; no formal policies. "Formal" means command and control policies are published and enforced
- Formal command and control SOPs address interoperability in planned and day-to-day events (e.g., vehicle pursuit, multiple station response) for agencies with which you provide joint incident response
- Formal command and control SOPs address interoperability during day-to-day, emergency, and out-of-the-ordinary events (e.g., mass casualties, flipped tanker that closes major highway) for agencies with which you provide joint incident response
- There is a review of interoperability command and control policies annually and after events that test organization capabilities

Are your agency's interoperability command and control policies NIMS-compliant?

Consider the questions to the left and how this measure varies across organizations, then choose one of these stages of development

☐	**Early Development** Some elements of formal command and control policies in practice
☐	**Moderate Development** Formal command and control policies in practice, but not consistent with command and control policies of all other necessary organizations
☐	**Full Development** NIMS-compliant command and control policies in practice consistent with all necessary organizations
☐	**Advanced Development** Annual review of command and control policies to assure continued compliance with NIMS and evaluation of command and control after significant events

Technology: Approaches

Approaches

How would you best describe the solutions first responders employ for interoperability?

- Portable, mobile, or temporary solutions developed in the field by first responders using resources/equipment on hand (e.g., radio swaps)
- Planned solution(s) are readily deployable, but do not employ mutually accepted equipment standards (e.g., communications vehicle)
- Permanent infrastructure-based solution(s) using mutually accepted equipment standards (e.g., shared system)
- Continuous technical improvements are planned that will develop networks that are completely transparent to responders

Consider the questions to the left and how this measure varies across organizations, then choose one of these stages of development

☐	**Early Development** Implementation of portable, mobile, or temporary solutions (ad hoc or COTS)
☐	**Moderate Development** Communications requirements exceed ad hoc capabilities, steps being taken toward permanent solutions
☐	**Full Development** Permanent infrastructure-based solutions using mutually accepted standards
☐	**Advanced Development** Strategic, coordinated communications plans in place to guide technical improvements that lead to seamless networks

Technology: Implementation

Implementation

How would you best describe the methods used by first responders to achieve interoperability?

— No consistent approach to solutions; first responders must improvise a solution

— Planned solution(s) require human intervention by someone other than first responders (e.g., must get patch through dispatcher)

— Solution(s) available to all first responders as authorized, without any intervention

— Piloting of advanced solution(s), technologies, and processes

Consider the questions to the left and how this measure varies across organizations, then choose one of these stages of development

☐	**Early Development** Ad hoc solutions
☐	**Moderate Development** Planned solutions that require human intervention
☐	**Full Development** Solutions available 24x7 without any intervention
☐	**Advanced Development** Research and testing of advanced solutions, technologies, and processes

Technology: Maintenance and Support

Maintenance and Support

How would you best describe the frequency and approach taken in communications equipment care, maintenance, repair, and systems lifecycle planning?

- There is either no maintenance or no consistent approach for preventive maintenance and interoperability equipment repair, replacement
- Plans guarantee minimum level of reliability and availability
- Plans guarantee capability to interoperate 24 x 7
- Near-term and long-term lifecycle planning (e.g., planning, acquisition, implementation, maintenance) of next solution

Consider the questions to the left and how this measure varies across organizations, then choose one of these stages of development

☐ **Early Development**

Ad hoc maintenance and equipment support

☐ **Moderate Development**

Plans developed plus staff and funding available to address maintenance and equipment support requirements

☐ **Full Development**

Multiple organizations' staff share maintenance and equipment support roles for jointly funded infrastructure through formal agreements

☐ **Advanced Development**

Near-term and long-term system lifecycle planning (e.g., planning, acquisition, implementation) and staffing

Training and Exercises: Operator Training

Training for Support Personnel

How would you best describe the nature of the education given to support personnel regarding interoperability?

- Support personnel (e.g., administrators, dispatchers, maintenance personnel) may have some awareness of interoperability, and some may have received informal education or training. Informal training has no lesson plans, may be on-the-job, and provides no assessment of student performance/change of behavior
- Some support personnel have received formal interoperability training (uses a lesson plan in a classroom or OJT setting, and includes an assessment of student performance/change of behavior either at the time of training or shortly thereafter)
- Substantially all support personnel have received formal interoperability training (as defined above)
- Organizations evaluate after-action reports, along with the changing operational environment, to adapt future training to address gaps and needs

Training for Field Personnel

How would you best describe the nature of the education given to field personnel regarding interoperability?

- Field personnel (e.g., law enforcement officers, firefighters, EMTs) may have some awareness of interoperability, and some may have received informal education or training. Informal training has no lesson plans, may be on-the-job, and provides no assessment of student performance/change of behavior
- Some field personnel have received formal interoperability training (uses a lesson plan in a classroom or OJT setting, and includes an assessment of student performance/change of behavior either at the time of training or shortly thereafter)
- Substantially all field personnel have received formal interoperability training (as defined above)
- Organizations evaluate after-action reports, along with the changing operational environment, to adapt future training to address gaps and needs

Consider the questions to the left and how this measure varies across organizations, then choose one of these stages of development

☐	**Early Development** No formal training in achieving interoperability
☐	**Moderate Development** Some organizations train regularly in using equipment and applying policies, practices, and procedures
☐	**Full Development** All necessary organizations participate in planned, regular training using equipment, policies, practices, and procedures, command and control, and NIMS
☐	**Advanced Development** Organizations evaluate training after-action reports and the changing operational environment to adapt future training to address gaps and needs

Training and Exercises: Exercises

Exercises

How would you best describe the simulated or in-field activities conducted to prepare responders for situations that would require interoperable communications?

- Your organization may have participated in planning workshops oriented toward interoperability
- Your organization participates in tabletop exercises, which incorporate interoperable communications, on a regular cycle
- Your organization participates in fully functional operational exercises, including interoperable communications, on a regular cycle
- Organizations evaluate after-action reports from fully functional exercises and in the changing operational environment to adapt exercises to address gaps and operational needs

Are your agency's interoperability exercises National Incident Management System (NIMS)-compliant?

Consider the questions to the left and how this measure varies across organizations, then choose one of these stages of development

☐	**Early Development** Some command and staff across organizations participate in workshops oriented to interoperability
☐	**Moderate Development** All necessary organizations participate in tabletop exercises; including NIMS; planned and on a regular cycle
☐	**Full Development** All necessary organizations participate in fully-functional operational exercises, including NIMS, on a planned and regular cycle
☐	**Advanced Development** Organizations evaluate after-action reports from the exercises and the changing operational environment to adapt exercises to address gaps and operational needs

Usage: Frequency of Use and Familiarity

Frequency of Use and Familiarity

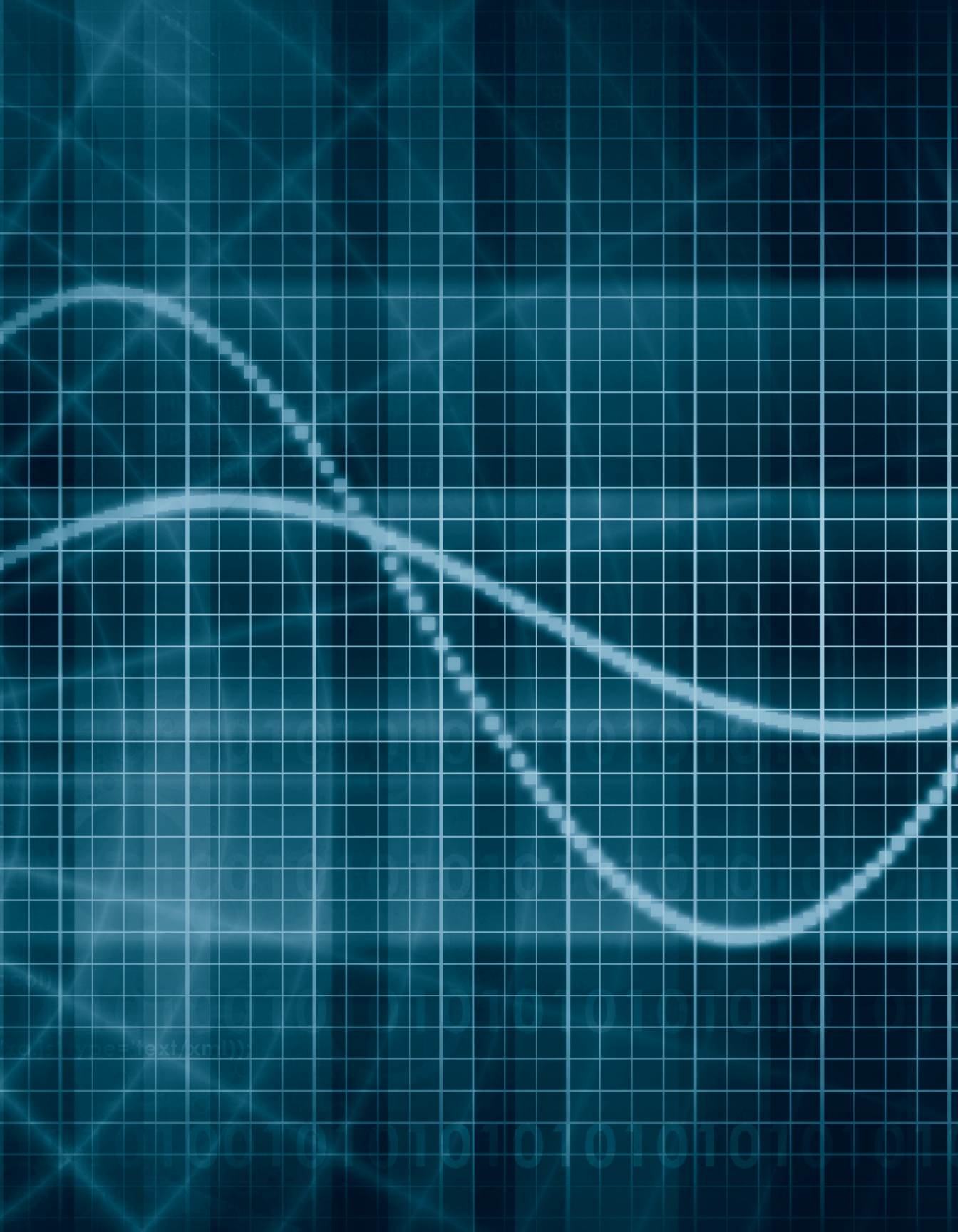
How would you best describe how frequently and easily your first responders use interoperability?

- First responders seldom use interoperability solutions, except for events that can be planned ahead of time
- First responders use solutions regularly for emergency events and to a limited extent for day-to-day communications
- First responders use solutions regularly and easily for all day-to-day, task force, and mutual aid events
- Regular use of completely transparent solutions has expanded to all potentially involved responders

Consider the questions to the left and how this measure varies across organizations, then choose one of these stages of development

☐	**Early Development** First responders seldom use solutions unless advanced planning is possible (e.g., special event)
☐	**Moderate Development** First responders use solutions regularly for emergency events, and in a limited fashion for day-to-day communications
☐	**Full Development** First responders use solutions regularly and easily for all day-to-day, task force, and mutual aid events
☐	**Advanced Development** Regular use of seamless solutions has expanded to include state, federal, and private responders

Appendix E: Bibliography and Resources



Appendix E:
Bibliography and Resources

ABI Research. "Mesh Network Market May See Tenfold Growth in Five Years." ABI Research press release, November 16, 2005. See **www.abiresearch.com/abiprdisplay.jsp?pressid=556**.

Advanced Generation of Interoperability for Law Enforcement. *Operational Test Bed—Alexandria (OTB-A) Communications Interoperability Gateway Subsystem Operational Test Document*, Report No. TE-00-04, 23. Rome, NY: National Law Enforcement and Corrections Technology Center-Northeast, July 23, 2001. See **www.safecomprogram.gov/library/Lists/Library/Attachments/257/Operational_Test_Bed.pdf**.

Atkinson, DJ. *Update on Public Safety Communications Intelligibility in High Background Noise*. Public Safety Communications Research Program. March 2009. See **www.pscr.gov/about_pscr/highlights/iwce_2010/iwce_2010_audio_20100310.pdf**.

Cisco Systems, Inc. "Wireless LANS – Total Cost of Ownership." 2004. See **www.customcable.com/wgcc/WhitePapers/CiscoTCO.pdf**.

Disaster Management Interoperability Services website. See **www.cmi-services.org**.

Dobkin, Daniel M. RF Engineering for Wireless Networks: Hardware, Antennas, and Propagation. Burlington, MA: Newnes, 2004.

Erlanger, Leon. "Building the intelligent network." *InfoWorld*, July 18, 2005. See **www.infoworld.com/reports/29SRintelnet.html**.

Federal Communications Commission, 700 MHz Interoperability Spectrum website. See **http://transition.fcc.gov/pshs/public-safety-spectrum/700-MHz/**.

Federal Communications Commission. *Connecting America: The National Broadband Plan (NBP)*. March 2010. See **www.broadband.gov/plan/**.

Federal Communications Commission. *A Glossary of Telecommunications Terms*. Washington, D.C.: 1998. See **http://web.archive.org/web/19980524230851/http://www.fcc.gov/Consumers/glossary.html**.

Global Infrastructure/Standards Working Group. *A Framework for Justice Information Sharing: Service-Oriented Architecture (SOA)*. December 9, 2004. See **http://it.ojp.gov/default.aspx?area=globalJustice&page=1235**.

Global Justice Information Sharing Initiative Advisory Committee. "Charter." October 15, 2002. See **http://it.ojp.gov/documents/GAC_Charter_2002.pdf**.

Harris, Kelly J., and William H. Romesburg. Law Enforcement Tech Guide: How to plan, purchase and manage technology (successfully!), A Guide for Executives, Managers and Technologists. Washington, D.C.: U.S. Department of Justice, Office of Community Oriented Policing Services, 2002. See **www.cops.usdoj.gov/files/ric/Publications/lawenforcementtechguide.pdf**.

Hawkins, Dan. *Communications in the Incident Command System*. Washington, D.C.: U.S. Department of Justice, Office of Community Oriented Policing Services, 2007. See **http://cops.usdoj.gov/files/ric/Publications/communicationsics.pdf**.

Homeland Security Presidential Directive/HSPD-5. "Management of Domestic Incidents." February 28, 2003. See **www.dhs.gov/xabout/laws/gc_1214592333605.shtm**.

Homeland Security Presidential Directive/HSPD-8. "National Preparedness." December 17, 2003. See **www.whitehouse.gov/news/releases/2003/12/20031217-6.html**.

Information Sharing Environment (ISE) website. See **www.ise.gov**.

Institute for Policy Research, Northwestern University. *Policing Smarter Through IT: Lessons in Enterprise Implementation.* Washington, D.C.: U.S. Department of Justice, Office of Community Oriented Policing Services, September 2004. See **www.cops.usdoj.gov/html/cd_rom/tech_docs/pubs/PolicingSmarterThroughITLessonsEnterprise.pdf**.

Institute for Security Technology Studies. *Crisis Information Management Software (CIMS) Interoperability: A Status Report.* Hanover, NH: Dartmouth College, October 2004. See **www.ists.dartmouth.edu/library/213.pdf**.

McKinsey & Company. *Improving NYPD Emergency Preparedness and Response*. August 19, 2002. See **www.mckinsey.com/locations/madrid/pdfs/nypdemergency.pdf**.

McKinsey & Company. *Increasing FDNY's Preparedness: Executive Summary*. August 19, 2002. See **www.nyc.gov/html/fdny/html/mck_report/toc.shtml**.

Metropolitan Emergency Services Board, St. Paul, Minnesota, "800 MHz Trunked Regional Public Safety Radio System Standards, Protocols, Procedures" (interim).

MissionCritical Communications. "Public Safety Report: Snapshot Survey – Wireless Networking." September 2005.

Montana Department of Administration, Public Safety Radio Communications Program. *Mutual Aid and Common Frequencies, 2005*. Helena, MT: June 2005. See **http://pssb.mt.gov/mutual_aid_manual.mcpx**.

National Commission on Terrorist Attacks Upon the United States. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. Washington, D.C.: U.S. Government Printing Office, July 2004. See **www.9-11commission.gov**.

National Emergency Number Association. *NENA Master Glossary of 9-1-1 Terminology*. NENA-01-002 Arlington, VA: November 29, 2005. See **www.nena.org/?page=Glossary**.

National Institute for Occupational Safety and Health (NIOSH), U.S. Department of Health and Human Services. *NIOSH Alert: Preventing Injuries and Death from Falls during Construction and Maintenance of Telecommunication Towers*. NIOSH Publication No. 2001-156. Cincinnati, OH: July 2001. See **www.cdc.gov/niosh/docs/2001-156/**.

National Task Force on Interoperability. Why Can't We Talk? Working Together to Bridge the Communications Gap to Save Lives, A Guide for Public Officials. February 2003. See **www.ncjrs.gov/pdffiles1/nij/204348.pdf**.

National Wildfire Coordinating Group Taskbooks. See **http://training.fema.gov/position%20specific%20taskbooks/taskbook_list.asp**.

Next Generation 9-1-1. See **http://transition.fcc.gov/pshs/services/911-services/nextgen.html** and **www.its.dot.gov/ng911/index.htm**.

Project Management Institute. *A Guide to the Project Management Book of Knowledge*, Fourth Edition. Newtown Square, PA: 2008.

Project MESA website. See **www.projectmesa.org**.

Public Safety Wireless Advisory Committee. *Final Report*. Presented to the Federal Communications Commission and the National Telecommunications and Information Administration, September 11, 1996.
See **www.ntia.doc.gov/legacy/osmhome/pubsafe/PSWAC_AL.pdf**.

Public Safety Wireless Network. LMR Replacement Cost Study Report. Prepared by Booz, Allen & Hamilton Inc., June 1998. See **www.safecomprogram.gov/library/lists/library/DispForm.aspx?ID=96**.

Public Safety Wireless Network. Public Safety Radio Spectrum: A Vital Resource for Saving Lives and Protecting Property. n.d. See **www.safecomprogram.gov/library/Lists/Library/Attachments/211/Public_Safety_Radio_Spectrum%20-%20A_Vital_Resource_for_Saving_Lives_and_Protecting_Property.pdf.**

Public Safety Wireless Network Program, Embedded Communications Broker (ECB) Technology, white paper, October 2001. See **http://permanent.access.gpo.gov/websites/safecomprogramgov/www.safecomprogram.gov/admin/librarydocs9/jill_ecb.pdf**.

Public Safety Wireless Network Program. Greenhouse Project Wideband Data Technology. White paper, September 2001. See **www.safecomprogram.gov/library/Lists/Library/Attachments/242/Greenhouse_Project.pdf.**

Public Safety Wireless Network Program. Public Safety In-Building/In-Tunnel Ordinances and Their Benefits to Interoperability Report. November 2002.
See **www.safecomprogram.gov/library/Lists/Library/Attachments/293/Public_Safety_In-Building_In-Tunnel_Ordinances.pdf.**

Public Safety Wireless Network Program Management Office. *PSWN Program Analysis of Fire and EMS Communications Interoperability*. Prepared by Booz, Allen & Hamilton Inc., April 1999. See **www.safecomprogram.gov/library/Lists/Library/Attachments/152/Fire_EMS_Interoperability_Study_Summary_Report.pdf**.

Roberts, David J. *Integration in the Context of Justice Information Systems: A Common Understanding*. Sacramento, CA: SEARCH Group, Incorporated, updated 2004.
See **www.search.org/files/pdf/Integration.pdf**.

Roberts, David J. *Law Enforcement Tech Guide for Creating Performance Measures that Work: A Guide for Executives and Managers*. U.S. Department of Justice, Office of Community Oriented Policing Services, 2006.
See **www.search.org/files/pdf/PMTechGuide.pdf**.

Romesburg, William H. *Law Enforcement Tech Guide for Small and Rural Police Agencies: A Guide for Executives, Managers, and Technologists*. Washington, D.C.: U.S. Department of Justice, Office of Community Oriented Policing Services, 2005. See **www.cops.usdoj.gov/files/RIC/Publications/e12051226_web.pdf**.

Ross, Ron, et al. *Recommended Security Controls for Federal Information Systems*, NIST SP 800-53. Washington, D.C.: U.S. Department of Commerce, National Institute of Standards and Technology, February 2005, including updates to June 17, 2005. See **http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final.pdf**.

San Francisco TechConnect website. See **www.sfgov.org/site/tech_connect_page.asp?id=33899**.

Signorini, Eugene. *3G Represents an Inflection Point for Enterprise Mobility*. Boston, MA: Yankee Group Research, Inc., 2004.

South Carolina Budget and Control Board, Division of the State Chief Information Officer. "Trunked 800 MHz System Interconnect Guidelines." See **http://cio.sc.gov/councilscommittees/palmetto800/**.

Stoneburner, Gary, Clark Hayden, and Alexis Feringa. *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*, NIST SP 800-27. Washington, D.C.: U.S. Department of Commerce, National Institute of Standards and Technology, June 2001. See **http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf**.

Swanson, Marianne, and Barbara Guttman. *Generally Accepted Principles and Practices for Security Information Technology Systems*. Washington, D.C.: U.S. Department of Commerce, National Institute of Standards and Technology, September 1996. See **http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf**.

Taylor, Mary J., et al. *State and Local Law Enforcement Wireless Communications and Interoperability: A Quantitative Analysis*, NCJ 168961. Washington, D.C.: U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, January 1998. See **www.ncjrs.gov/pdffiles1/168961.pdf**.

Titan Systems Corp. Arlington County Virginia After-Action Report on the Response to the September 11 Terrorist Attack on the Pentagon. Arlington, VA: n.d.. See **www.floridadisaster.org/publications/Arl_Co_AAR.pdf**.

U.S. Department of Homeland Security. *National Infrastructure Protection Plan (NIPP)*. 2009. See **www.dhs.gov/files/programs/editorial_0827.shtm**.

U.S. Department of Homeland Security. *National Incident Management System*. December 2008. See **www.fema.gov/pdf/emergency/nims/NIMS_core.pdf**.

U.S. Department of Homeland Security. *National Preparedness Guidelines*. September 2009. See **www.dhs.gov/xlibrary/assets/National_Preparedness_Guidelines.pdf**.

U.S. Department of Homeland Security. *National Response Framework (NRF)*. See **www.fema.gov/NRF**.

U.S. Department of Homeland Security, Office of Emergency Communications. *Communications Interoperability Performance Measurement Guide*. April 2011. See **www.safecomprogram.gov/SiteCollectionDocuments/OECPerformanceMeasurementGuide.pdf.**

U.S. Department of Homeland Security, Office of Emergency Communications. *Emergency Communications System Life Cycle Planning Guide*. August 2011. See **www.safecomprogram.gov/library/lists/library/DispForm.aspx?ID=324**.

U.S. Department of Homeland Security, Office of Emergency Communications. *National Emergency Communications Plan*. July 2008. See **www.dhs.gov/xlibrary/assets/national_emergency_communications_plan.pdf**.

U.S. Department of Homeland Security, Office of Emergency Communications. *The Public Safety Communications Evolution*. November 2011. See **www.safecomprogram.gov/library/lists/library/DispForm.aspx?ID=330**.

U.S. Department of Homeland Security, Office of Emergency Communications. "OEC Guidance Documents." See **www.safecomprogram.gov/oecguidancedocuments/webpages/ts.aspx**.

U.S. Department of Homeland Security, Office of Grants and Training, "HSPD-8 Overview." See **www.dhs.gov/xabout/laws/gc_1215444247124.shtm**.

U.S. Department of Homeland Security, Office of State and Local Government Coordination and Preparedness, Office for Domestic Preparedness. *Fiscal Year 2005 Homeland Security Grant Program: Program Guidelines and Application Kit*, version 2. Washington, D.C.: December 22, 2004. See **www.fema.gov/pdf/government/grant/hsgp/fy05_hsgp_guidance.pdf**.

U.S. Department of Homeland Security, SAFECOM Program. *National Interoperability Baseline Survey*. December 2006.
See **www.safecomprogram.gov/baseline/Default.aspx**.

U.S. Department of Homeland Security, SAFECOM Program. *National Summary of Statewide Interoperability Communications Plans (SCIPs)*. February 2009.
See **www.safecomprogram.gov/SiteCollectionDocuments/NationalSummaryofSCIPs_February2009.pdf**.

U.S. Department of Homeland Security, SAFECOM Program. *Project 25 Compliance Assessment Program (CAP)*.
See **www.safecomprogram.gov/currentprojects/project25cap/Default.aspx**.

U.S. Department of Homeland Security, SAFECOM Program. *Statement of Requirements for Public Safety Wireless Communications and Interoperability*. Washington, D.C.: Volume I, Version 1.2, October 2006. See **www.safecomprogram.gov/library/Lists/Library/Attachments/302/Statement_of_Requirements_Volume_I%20-%20Version%201_2.pdf**.

U.S. Department of Homeland Security, SAFECOM Program. *Statement of Requirements for Communications and Interoperability*. Washington, D.C.: Volume II, Version 1.2, August 2008.
See **www.safecomprogram.gov/library/Lists/Library/Attachments/302/Statement_of_Requirements_Volume_II%20-%20Version%201_2.pdf**.

U.S. Department of Justice, National Institute of Justice. "What's New from CommTech."
See **www.nij.gov/nij/topics/technology/communication/welcome.htm**.

U.S. Department of Justice, Office of Justice Programs, Information Technology Initiatives. "Global Justice XML Data Model." See **www.it.ojp.gov/gjxdm**.

U.S. Department of Justice, Office of Justice Programs, Information Technology Initiatives. "Global JXDM Implementation Guidelines."
See **http://it.ojp.gov/topic.jsp?topic_id=138**.

U.S. Department of Justice, Office of Justice Programs, Justice Information Sharing. "Global Reference Architecture (GRA)."
See **http://it.ojp.gov/default.aspx?area=nationalInitiatives&page=1015**.

U.S. General Accounting Office. *Homeland Security: Challenges in Achieving Interoperable Communications for First Responders*. Testimony before the subcommittees of the Government Reform Committee, House of Representatives, GAO 04-231T. Washington, D.C.: November 6, 2003. See **www.gao.gov/new.items/d04231t.pdf**.

U.S. Government Accountability Office. Homeland Security: Federal Leadership and Intergovernmental Cooperation Required to Achieve First Responder Interoperable Communications, GAO-04-740. Washington, D.C.: July 2004.

Vandereau, John M. *Delivered Audio Quality Measurements on Project 25 Land Mobile Radios*, NTIA Report 99-358. Washington, D.C.: U.S. Department of Commerce, Institute for Telecommunications Science, 1998.
See **www.its.bldrdoc.gov/pub/ntia-rpt/99-358**.

WebSite Optimization.com. "US Broadband Breaks 60% among Active Internet Users, but growth slows." September 2005.
See **www.websiteoptimization.com/bw/1002**.

WiMAX Forum. "About the WiMAX Forum." See **www.wimaxforum.org/about**.

Wireless Philadelphia Executive Committee website. See **www.wirelessphiladelphia.net/**.

Wisconsin Department of Justice, Division of Law Enforcement Services, Crime Information Bureau. "eTIME Project." See **www.doj.state.wi.us/les/TIME/eTIME.htm**.

Additional Resources

800 MHz Transition Administrator. See **www.800ta.org**.

Association of Public-Safety Communications Officials – International, Inc. (APCO) Interoperability Resources. See **www.apcointl.org/frequency/interoperability.php**.

Automated Frequency Coordination, Inc., a subsidiary of APCO.
See **www.apcointl.org/frequency/**.

California Tactical Dispatcher Association. See **www.tacticaldispatch.com**.

Cover Pages (hosted by OASIS), Emergency Data Exchange Language (EDXL).
See **http://xml.coverpages.org/edxl.html**.

FCC (Federal Communications Commission), 700 MHz Public Safety Spectrum page.
See **http://transition.fcc.gov/pshs/public-safety-spectrum/700-MHz/**.

FCC, 800 MHz Band Reconfiguration page. See **http://wireless.fcc.gov/publicsafety/800MHz/bandreconfiguration/index2.html**.

FCC, Public Safety Frequency Coordinators page.
See **http://wireless.fcc.gov/publicsafety/coord.html**.

FCC, Interoperability Spectrum page.
See **http://transition.fcc.gov/pshs/public-safety-spectrum/700-MHz/**.

FCC, Refarming page. See h**ttp://wireless.fcc.gov/services/plmrs/refarming/**.

FCC, Special Temporary Authority page.
See **http://transition.fcc.gov/pshs/services/sta.html**.

Global Justice XML Data Model (GJXDM) Introduction page.
See **http://it.ojp.gov/jxdm/**.

Hawaii State Government Internet portal demonstration video.
See **www2.hawaii.gov/dags/icsd/content/video/higovdemo_250k.asf.**

IEEE (Institute of Electrical and Electronics Engineers) 802.11 series of standards.
See **www.ieee802.org/11**.

IEEE 802.16 Working Group on Broadband Wireless Access Standards. See **www.ieee802.org/16**.

Incidentdispatch.net. See **www.incidentdispatch.net**.

Internet Engineering Task Force (IETF). See **www.ietf.org**.

Law Enforcement Information Technology Standards Council (LEITSC). See **www.theiacp.org/Technology/OperationalTechnologies/CADRMS/tabid/831/Default.aspx**.

Los Angeles Regional Tactical Radio Communications System (LARTCS). See **www.lartcs.org**.

Louisville (Kentucky) Metro's MetroSafe (emergency communications network). See **www.louisvilleky.gov/MetroSafe**.

Metropolitan Emergency Services Board, St. Paul, Minnesota. See **www.mn-mesb.org**.

Minnesota Department of Public Safety, Allied Radio Matrix for Emergency Response (ARMER). See **www.armer.state.mn.us**.

National Association of Tower Erectors (NATE). See **www.natehome.com**.

National Information Exchange Model (NIEM). See **www.niem.gov**.

National Information Exchange Model (NIEM). *How to Use NIEM to Build IEPDs*. See **www.niem.gov/faq/Pages/how-do-i-use-niem-to-build-iepds.aspx**.

National Information Exchange Model (NIEM). *IEPD Clearinghouse*. See **http://it.ojp.gov/default.aspx?area=implementationAssistance&page=1108**.

National Interagency Incident Communications Division (NIICD). See **www.nifc.gov/NIICD/index.html**.

National Public Safety Telecommunications Council (NPSTC). See **www.npstc.org/siec.jsp**.

National Security Agency, Central Security Service, Information Assurance Directorate page on TEMPEST. See **www.nsa.gov**.

National Task Force on Interoperability. *Supplemental Resources* to "Why Can't We Talk? Working Together to Bridge the Communications Gap To Save Lives." February 2003. See **www.iafc.org/files/commComm_ntfi_supplementalLowRes.pdf**.

National Wildfire Coordinating Group (NWCG). See **www.nwcg.gov**.

NIMSonline.com, serving the National Incident Management System community, examples of ICS forms page.
See **www.fema.gov/pdf/emergency/nims/ics_forms_2010.pdf**.

North Central Texas Council of Governments. See **www.nctcog.org**.

Open Systems Interconnection model.
See **http://en.wikipedia.org/wiki/Open_Systems_Interconnection**.

Organization for the Advancement of Structured Information Standards (OASIS).
See **www.oasis-open.org**.

Project 25 Technology Interest Group. See **www.project25.org**.

SAFECOM Program of the Department of Homeland Security.
See **www.safecomprogram.gov**.

SAFECOM Program, grant guidance page for interoperability projects.
See **www.safecomprogram.gov/grant/Default.aspx.**

SEARCH Group, Incorporated and U.S. Department of Justice, Bureau of Justice Assistance. *Building Exchange Content Using the Global Justice XML Data Model: A User Guide for Practitioners and Developers*. June 2005.
See **http://it.ojp.gov/documents/GJXDMUserGuide.pdf**.

SEARCH, Information Exchange Package Documentation project.
See **www.search.org/programs/info/publications/**.

SEARCH Group, Incorporated. *Project Planning Resource Toolkit*. 2011.
See **www.search.org/files/doc/Project-Planning-Resource-Toolkit.docx**.

SEARCH, Workshop Report: Law Enforcement Information Exchange Package Documentation, Constructed from GJXDM 3.0.2. March 15, 2005.
See **www.search.org/files/pdf/gjxdm-iep.pdf**.

Skydrive document sharing and storage tool.
See **http://explore.live.com/skydrive-get-started**.

South Carolina Budget and Control Board, Division of the State Chief Information Officer, Palmetto 800 Radio System page.
See **http://cio.sc.gov/councilscommittees/palmetto800/**.

Telecommunications Industry Association (TIA). See **www.tiaonline.org**.

U.S. Department of Homeland Security, Lessons Learned Information Sharing site (requires registration). See **www.llis.dhs.gov**.

U.S. Department of Homeland Security, Office for Domestic Preparedness, Homeland Security Exercise and Evaluation Program (HSEEP).
See **https://hseep.dhs.gov/pages/1001_HSEEP7.aspx**.

U.S. Department of Homeland Security, Office for Domestic Preparedness. *Homeland Security Exercise and Evaluation Program, Volume III: Exercise Evaluation and Improvement*, NCJ 202198. Washington, D.C.: October 2003.
See **https://hseep.dhs.gov/pages/1001_HSEEP7.aspx**.

U.S. Department of Homeland Security, Office of Grants and Training, Interoperable Communications Technical Assistance Program (ICTAP) page.
See **www.dhs.gov/files/training/gc_1287084689081.shtm**.

U.S. Department of Homeland Security, SAFECOM Program.
Communications Specific Tabletop Exercise Methodology.
See **www.safecomprogram.gov/SiteCollectionDocuments/CommunicationsSpecificTabletopExerciseMethodology.pdf**.

U.S. Department of Homeland Security, SAFECOM Program. *Interoperability Continuum*. See **www.safecomprogram.gov/oecguidancedocuments/continuum/Default.aspx**.

U.S. Department of Homeland Security, SAFECOM Program, Library.
See **www.safecomprogram.gov/library/default.aspx**.

U.S. Department of Homeland Security, SAFECOM Program, Public Safety Wireless Network. *Comparisons of Conventional and Trunked Systems*. May 1999.
See **www.safecomprogram.gov/library/Lists/Library/DispForm.aspx?ID=239**.

U.S. Department of Homeland Security, SAFECOM Program, Public Safety Wireless Network Program. *How 2 Guide for Establishing and Managing Talk Groups*. n.d. See **www.safecomprogram.gov/library/Lists/Library/Attachments/216/How_to_Establish_and_Manage_Talk_Groups.pdf**.

U.S. Department of Homeland Security, SAFECOM Program, Public Safety Wireless Network Program. *Introduction to Encryption Key Management for Public Safety Radio Systems*. October 2001. See **www.safecomprogram.gov/library/Lists/Library/Attachments/208/Security_Issues_and_Analysis_Report%20-%20Encryption_Key_Management.pdf**.

U.S. Department of Homeland Security, SAFECOM Program, Public Safety Wireless Network Program. *Key Management Plan Template for Public Safety Land Mobile Radio Systems*. February 2002.
See **www.safecomprogram.gov/library/Lists/Library/DispForm.aspx?ID=202**.

U.S. Department of Homeland Security, SAFECOM Program, Public Safety Wireless Network Program. *Operational Best Practices for Managing Trunked Land Mobile Radio Systems*. May 2003.
See **www.safecomprogram.gov/library/Lists/Library/DispForm.aspx?ID=219**.

U.S. Department of Homeland Security, SAFECOM Program, Public Safety Wireless Network Program. "Public Safety's New Allocation—Answering Users' Questions on the 4.9 Gigahertz Band." n.d. See **www.safecomprogram.gov/library/Lists/Library/Attachments/212/Public_Safetys_New_Allocation.pdf**.

U.S. Department of Homeland Security, SAFECOM Program, Public Safety Wireless Network Program. *Software-Enabled Wireless Interoperability Assessment Report – Voice-Over-Internet Protocol Technology*. December 2001. See **www.safecomprogram.gov/library/Lists/Library/Attachments/300/VoIP_Technology_Assessment.pdf**.

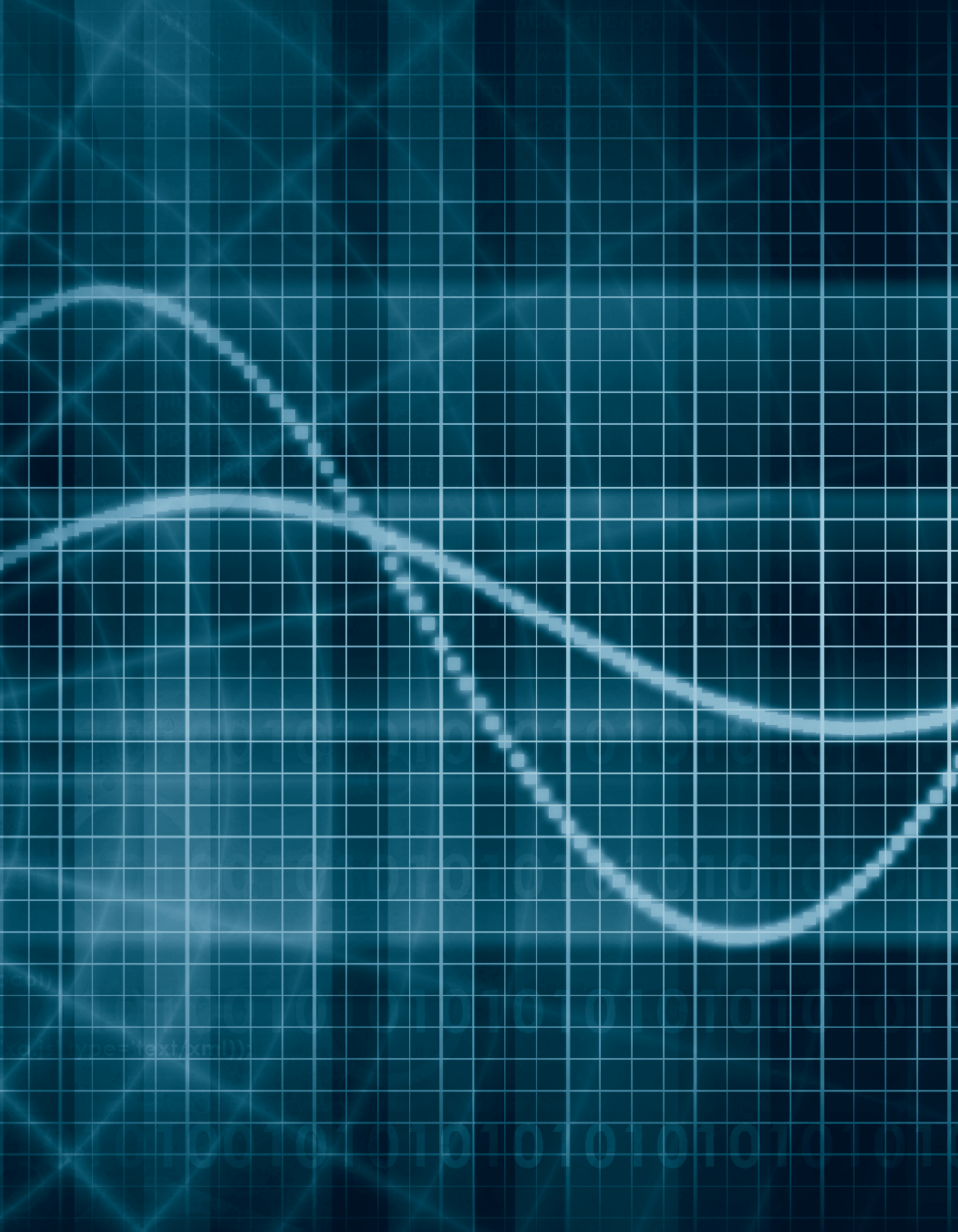
U.S. Department of Justice Office of Community Oriented Policing Services. *Summit on Implementing Wireless Communications: Perspectives on Interoperability from the Law Enforcement Community*. See **www.cops.usdoj.gov/Default.asp?Item=1495**.

Virginia Interoperability site. See **www.vahs.virginia.gov**.

Washington State's Statewide Interoperability Executive Committee.
See **http://isb.wa.gov/committees/siec/**.

Wi-Fi Alliance. See **www.wi-fi.org**.

Appendix F:
Glossary



Appendix F:
Glossary

1xEv-DO
Formally, CDMA2000 1xEv-DO (Evolution – Data Optimized), a CDMA2000 technology. The "1x" refers to use of a single pair of 1.25 MHz radio channels. Carrier reported data rates are in the 300 Kbps to 1.2 Mbps range. Considered to be a 3G wireless service. Also known as "EvDO."

1xRTT
Formally, CDMA2000 1xRTT (Radio Transmission Technology), a CDMA2000 technology. The "1x" refers to use of a single pair of 1.25 MHz radio channels. Carrier reported data rates are in the 50 to 200 Kbps range. Considered to be a 2.5G wireless service.

1G, 2G, 3G, 4G, etc.
Successive generations of wireless telephone technologies. The first generation is commonly considered to be analog cellular telephony.

3GSM
See *Universal Mobile Telecommunications System* (UMTS).

ALI
See *Automatic Location Identification*.

ANI
See *Automatic Number Identification*.

Acceptance testing (COPS Law Enforcement Tech Guide)
The process that an agency uses to verify that the delivered and installed product meets requirements specified in the procurement documents and contract, particularly regarding functionality, reliability, and performance.

Ad hoc working groups (COPS Law Enforcement Tech Guide)
Groups that are formed as a subset to the project's formal decision-making structure to look at specific tasks and business processes that require more in-depth research or analysis, or to carry out research on and development of a variety of project-specific plans, models, policies, and directions. Assembled on a temporary basis to address a specific issue or task.

Advanced Generation of Interoperability for Law Enforcement (AGILE) (NTFI Guide – Glossary of Terms)
The AGILE Program was created in 1998 to group together all of the interoperability projects [then] underway at the National Institute of Justice.

Analog radio system (NTFI Guide – Glossary of Terms)
A radio system in which voice signals are sent over-the-air in an unaltered form and are heard in the same time frame over which they were communicated. (The human voice is an analog signal.) Cellular phones and other wireless devices still use analog in geographic areas where there is little or no coverage by digital networks.

Antenna (NTFI Guide – Glossary of Terms)
Any structure or device used to collect or radiate electromagnetic waves.

Association of Public-Safety Communications Officials International, Inc. (APCO) (NTFI Guide – Glossary of Terms)
APCO International is the world's oldest and largest not-for-profit professional organization dedicated to the enhancement of public safety communications.

Assumptions and constraints (COPS Law Enforcement Tech Guide)
Circumstances and events that can affect the success of the project and are generally out of the control of the project team. Include in the project charter to provide assistance in making/justifying decisions. Consult also when developing the project timeline and risk management plan.

Automatic Location Identification (ALI) (NENA Master Glossary)
The automatic display at the public safety answering point (PSAP) of the caller's telephone number, the address/location of the telephone, and supplementary emergency services information.

Automatic Number Identification (ANI) (NENA Master Glossary)
Telephone number associated with the access line from which a call originates.

Automatic Vehicle Location (AVL) software (COPS Law Enforcement Tech Guide)
Used by law enforcement agencies to remotely track the location of agency units via satellite global positioning systems (GPS). AVL combines GPS technology, wireless communications, street-level mapping, and a user interface.

Band (NTFI Guide – Glossary of Terms)
In communications, the spectrum between two defined limited frequencies. For example, the Ultra High Frequency (UHF) is located from 300 MHz to 3,000 MHz in the radio frequency spectrum.

Bandwidth (NTFI Guide – Glossary of Terms)
The size of a network "pipe" or channel for communications in wired networks. In wireless communications, it refers to the range of available frequencies that can carry a signal. In analog communications, bandwidth is typically measured in Hertz (cycles per second). In digital communications, bandwidth is typically measured in bits per second (bps).

Best practices (COPS Law Enforcement Tech Guide)
Industry-proven processes or methods that, when executed effectively, lead to enhanced or superior project performance and ensure the success of an undertaking (such as planning, procurement, implementation, and management).

Bluetooth
An open standard for short range, low-speed wireless networking intended to be used in computing and telecommunications equipment to replace cabling. It has an application in personal area networks (PANs) and is used popularly with wireless telephone headsets.

Bonding (COPS Law Enforcement Tech Guide)
Bonds required may include those dealing with performance, maintenance, and payment.

Broadband (FCC Glossary of Telecommunications Terms)
Broadband is a descriptive term for evolving digital technologies that provide consumers with a signal switched facility offering integrated access to voice, high-speed data service, video-demand services, and interactive delivery services.

Business case (COPS Law Enforcement Tech Guide)
The project's marketing plan that articulates why the project is important in terms of operational benefits to the agency, the justice system in general, and the public. Used to educate and inform all project stakeholders.

Business process (COPS Law Enforcement Tech Guide)
A written description of the things that employees do every day in their job functions assessed on a what, why, when, how, and where basis. Business processes are what technology seeks to enhance or improve.

CDMA
Code Division Multiple Access. A method of multiple access to a digital communications channel. In the wireless telephony environment, data bits from multiple voice channels are spread across a wide radio channel simultaneously.

cdmaOne
The first CDMA technology for mobile digital telephony based on the TIA/EIA-95 standard, previously known as Interim Standard 95 (IS-95). cdmaOne™ is a trademark of the CDMA Development Group, Inc. Considered to be a 2G wireless service.

CDMA2000
A CDMA technology for mobile digital telephony and data based on the TIA Interim Standard 2000 (IS-2000). The term encompasses multiple CDMA data technologies, including 1xRTT and EVDO (See *1xEv-DO* entry). CDMA2000® is a registered trademark of the Telecommunications Industry Association (TIA).

Cellular Digital Packet Data (CDPD)
A wireless, packet data service operated on analog or 1G cellular systems. Provided data rates of approximately 19.2 Kbps. Originally available in the mid-1990s and widely available by 2000. Major carriers transitioned out of CDPD in 2004 to 2005.

Channel (NTFI Guide – Glossary of Terms)
A single unidirectional or bidirectional path for transmitting or receiving, or both, of electrical or electromagnetic signals.

Client-server (COPS Law Enforcement Tech Guide)
An application that runs on a personal computer or workstation and relies on a server to perform some operations. A thin client is a client designed to be especially small so the bulk of data processing occurs on the server.

Commercial services (NTFI Guide – Glossary of Terms)
Communications services (e.g., cellular telephone and paging communications companies) run by private companies. Many public safety agencies use commercial services in their day-to-day operations.

Common carrier (FCC Glossary of Telecommunications Terms)
In the telecommunications arena, the term used to describe a telephone company.

Communications plan (COPS Law Enforcement Tech Guide)
Formal and agreed-upon strategies for communicating project status and activities to key stakeholders, and methods for developing historical project records and archives.

Communications system (NTFI Guide – Glossary of Terms)
A collection of individual communications networks, transmission systems, relay stations, tributary stations, and data terminal equipment usually capable of interconnection and interoperation to form an integrated whole. Note: The components of a communications system serve a common purpose, are technically compatible, use common procedures, respond to controls, and operate in unison.

Computer-aided Dispatch (CAD) System (COPS Law Enforcement Tech Guide)
Fully automates the call-taking and dispatching functions of a law enforcement agency and initiates and manages dispatch and incidents.

Contingency costs (COPS Law Enforcement Tech Guide)
Funding that is set aside for unexpected and, therefore, often unbudgeted activities. On average, contingencies range from 10 to 15 percent of the hardware and software costs.

Conventional radio system (NTFI Guide – Glossary of Terms)
A land mobile radio (LMR) system architecture similar to a telephone party line in that the user determines availability by listening for an open channel before transmitting.

Coverage (NTFI Guide – Glossary of Terms)
The geographic area included within the range of a wireless radio system.

Data (NTFI Guide – Glossary of Terms)
Representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. Any representations such as characters or analog quantities to which meaning is or might be assigned.

Day-to-day interoperability (FCC PSWAC Final Report)
This most frequent type of interoperability is commonly used in areas of concurrent jurisdiction where agencies need to monitor each other's routine communications. This minimizes the need for dispatcher-to-dispatcher interaction in exchanging information among field units. Interoperability is difficult to implement unless all equipment operates in the same frequency band and within the same type of infrastructure.

Dead spots (or zones) (NTFI Guide – Glossary of Terms)
The area, zone, or volume of space that is within the expected range of a radio signal, but in which the signal is not detectable and therefore cannot be received. Common causes of dead spots include depressions in the terrain and physical structures.

Decision-making structure (COPS Law Enforcement Tech Guide)
A group of agency staff that provides leadership and accountability; defines the business of the agency; analyzes technical environments, policies, and solutions; and effectively manages projects. Requires participation from three key representative groups within an agency: executive, business or operational, and technical.

Deliverable (COPS Law Enforcement Tech Guide)
A measurable, tangible, verifiable outcome that must be produced to complete a project or part of a project.

Digital (signal) (NTFI Guide – Glossary of Terms)
A signal in which discrete steps are used to represent information.

Digital radio system (NTFI Guide – Glossary of Terms)
A radio system where voice is converted to a digital format before being sent over the air. When the digital signal reaches the receiving radio, it is converted back to analog so that it is intelligible to the human ear. The benefit of digital radio systems is that the signal can be reproduced precisely.

EDGE
Enhanced Data Rates for GSM Evolution. A digital wireless technology providing high-speed data on GSM and other Time Division Multiple Access (TDMA) networks. EDGE services are designed to complement general packet radio systems (see *GPRS*). Carrier reported data rates are in the 50 to 200 Kbps range. Currently considered to be a 2.5G wireless service, but capable of being extended to higher speeds.

Electronic Industry Alliance (EIA)
EIA is a national (U.S.) trade organization of electronic and other high-technology organizations and companies that develops standards.

Environmental scan (ES) (COPS Law Enforcement Tech Guide)
An initial step in the planning process that helps the project team gain perspective on the initiative by allowing the team to systematically assess factors that present opportunities or threats to the success of the project. Sometimes referred to as a situation or "SWOT" assessment, an ES contains an internal scan that identifies strengths (S) and weaknesses (W) of the agency and an external scan that identifies external opportunities (O) and threats (T) to the agency.

EvDO
See *1xEv-DO*.

Executive sponsor (COPS Law Enforcement Tech Guide)
The individual who has the ultimate accountability for the project, having authority to sanction the project and make it a priority. Serves as the project's ultimate decision making authority.

Extended Area Network (EAN)
A basic communications networking type used to describe voice and/or data networks used by public safety agencies for both routine operations and emergencies. An EAN is the single or set of networks providing communications between agencies over an extended geographic expanse. Such a network used for data communications is also known as a wide area network (WAN) or extranet.

Extensible Markup Language
See *XML*.

Federal Communications Commission (FCC) (NTFI Guide – Glossary of Terms)
An independent federal agency that regulates U.S. broadcast media and communications markets, as well as local and state radio spectrum needs.

Federal Law Enforcement Wireless Users Group (FLEWUG)
(NTFI Guide – Glossary of Terms)
FLEWUG began as an ad hoc group of federal radio spectrum users that met to address the National Telecommunications and Information Administration's (NTIA) mandate for digital narrow-banding by 2005. The FLEWUG was formalized as a mechanism to address interoperability and other challenges related to public safety communications. The FLEWUG issued the Public Safety Wireless Network (PSWN) Program Management and Organization document in 1996, which led to the creation of the PSWN Program.

Fee-for-service (NTFI Guide – Glossary of Terms)
An arrangement in which a vendor has expended its own capital to build, install, administer, and maintain its own system for lease to public safety organizations.

Focus groups (COPS Law Enforcement Tech Guide)
A somewhat informal technique that can help to assess user needs while designing the system. Usually six to nine users gather to discuss issues and concerns about the features of the new system.

Frequency (NTFI Guide – Glossary of Terms)
For a periodic function, the number of cycles or events per unit time.

Frequency bands (NTFI Guide – Glossary of Terms)
Frequency bands where land mobile radio systems operate in the United States, including the following: High HF (25-29.99 MHz), Low VHF (30-50 MHz), High VHF (150-174 MHz), Low UHF (450-470 MHz), UHF TV Sharing (470-512 MHz), 700 MHz (764-776/794-806 MHz), and 800 MHz (806-869 MHz).

Frequency Modulation (FM) (FCC Glossary of Telecommunications Terms)
A signaling method that varies the carrier frequency in proportion to the amplitude of the modulating signal.

Functional specifications (COPS Law Enforcement Tech Guide)
Precise descriptions of how a product should operate. These statements should be succinct. A project plan and procurement document often contains numerous such functional requirements. During procurement, vendors should be required to divulge how closely their product matches an agency's functional specifications.

Functionality testing (COPS Law Enforcement Tech Guide)
A type of acceptance testing designed to ensure that the vendor's software is functioning as described in product literature and, possibly, in their response to the agency's RFP.

General Packet Radio System (GPRS)
A digital wireless technology providing high-speed data on GSM and other TDMA networks. Carrier reported data rates are in the 30 to 80 Kbps range. Considered to be a 2.5G wireless service.

Global System for Mobile (GSM) Communications
A worldwide standard for mobile digital telephony using TDMA channel access means for eight voice channels across wide (200 kHz) radio channels. Considered to be a 2G wireless service.

Gateway
In general telecommunications, a gateway is a device that connects two or more different networks. The term has come to mean more in land mobile radio communications where it is used in reference to several means of achieving technical interoperability in which independent systems are connected together so traffic on one channel, typically, of an agency's system is duplicated on another agency's channel. This is commonly done by electronic patching of transmit and receive audio of one channel to another, either at a dispatch console, separate radio sites, or in a mobile communications vehicle.

Gigabits/second (Gbps)
A measure of data transfer rates equal to one thousand megabits or one billion bits per second.

GJXDM
Global Justice XML Data Model. A data reference model for use with XML-based information exchange in justice and public safety applications.

Global Positioning System (GPS) (FCC Glossary of Telecommunications Terms)
A U.S. satellite system that lets those on the ground, on the water, or in the air determine their position with extreme accuracy using GPS receivers.

Global Reference Architecture (GRA)
The GRA is primarily intended to provide the bulk of what agencies and jurisdictions need to implement SOA in their environment, from technical specifications to setting up proper governance to acquiring the right technology infrastructure.

Hertz (Hz) (NTFI Guide – Glossary of Terms)
A unit of frequency in cycles per second. A hertz is one cycle per second.

Holdbacks (COPS Law Enforcement Tech Guide)
A contract provision that allows an agency to keep a percentage of a vendor's payment until after the vendor successfully completes certain milestones. Useful for keeping the vendor interested in completing all of the tasks associated with a project, even those that are less profitable than others.

Hotspot
In data networking usage, a wireless local area network (WLAN) access point offering network connections beyond.

ICS
See *Incident Command System*.

Integrated Digital Enhanced Network (iDEN)
A mobile digital telephony system first introduced in 1994, which uses TDMA channel access means to provide up to six voice channels across 25 kHz radio channels. Considered to be a 2G wireless service. iDEN™ is a trademark of Motorola, Inc.

Implementation plan (COPS Law Enforcement Tech Guide)
The blueprint that enables project management to define the rules that govern how technology will be installed, tested, and managed.

Incident Area Network (IAN)
A basic communications networking type used to describe voice and/or data networks used by public safety agencies for emergency incidents or events. An IAN is the single or set of networks providing communications for responders across the entire organization and geographic scope of an incident or event. Most commonly, an IAN is considered the collection of subnetworks used for a particular incident.

Incident Command System (ICS)
An organizational management system adapted from military techniques for public safety emergency response. It provides common terminology, modular organizational structures, and objectives-based management principles among its basic principles.

Infrastructure (NTFI Guide – Glossary of Terms)
When relating to radio communications systems, the hardware and software needed to complete and maintain the system.

Initial costs (COPS Law Enforcement Tech Guide)
One-time expenses to purchase technology and services for a project. Must be considered in conjunction with recurring costs (see *Recurring Costs*).

Integration
The ability to access and exchange critical information at key decision points throughout the enterprise.

Interference (NTFI Guide – Glossary of Terms)
In general, extraneous energy, from natural or manmade sources, that impedes the reception of desired signals.

Internal costs (COPS Law Enforcement Tech Guide)
Those costs over which your agency has direct financial responsibility and control, including personnel costs, infrastructure costs, cost recovery fees, etc.

Internet Protocol (IP)
One of a suite of protocols used to control exchange of data across systems and networks. IP and associated protocols are the common protocols that allowed standardization of computer networks, resulting in the Internet. Today, IP is the most common data networking protocol. The term is also used to refer to the entire suite of protocols commonly used across the Internet and private data networks.

Interconnects
See *Gateway*.

Intergovernmental Agreement (IGA)
A written agreement entered into between two or more public agencies that may be more or less formal depending on legal requirements on the agencies. Also known as an *interlocal agreement* (ILA) and used in some regions synonymously with the terms *memorandum of agreement* (MOA) or *understanding* (MOU).

Interoperability
The ability of public safety responders to share information via voice and data communications systems on demand, in real time, when needed, and as authorized.

Interstate Compact Agreement (NTFI Guide – Glossary of Terms)
A written contract between states to cooperate on a policy issue or program that extends across and through state boundaries.

Joint Powers Act (JPA) (NTFI Guide – Glossary of Terms)
A written contractual agreement entered into between two or more public agencies subject to any constitutional or legislative restriction imposed upon any of the contracting public agencies.

Jurisdiction Area Network (JAN)
A basic communications networking type used to describe voice and/or data networks used by public safety agencies for both routine operations and emergencies. A JAN is the single or set of networks providing communications for an agency across the organizational and geographic scope of its jurisdiction. It may be a shared network between agencies with overlapping geographic scopes of responsibility.

Kilobits/second (Kbps or kbps)
A measure of data transfer rates equal to one thousand bits per second.

Kilohertz (kHz) (NTFI Guide – Glossary of Terms)
A unit of frequency denoting one thousand Hz.

Land Mobile Radio (LMR) (NTFI Guide – Glossary of Terms)
A radio system that allows for wireless communications between base stations and land mobile stations (mobile or portable radios) or between land mobile stations.

Landline (FCC Glossary of Telecommunications Terms)
Traditional wired telephone service.

Lifecycle costing methods (COPS Law Enforcement Tech Guide)
Methods to determine the total cost of owning the technology, from procurement through upgrade and/or replacement.

Local Area Network (LAN)
A geographically and functionally constrained network connecting personal computers, servers, and printers.

Master Street Address Guide (MSAG) (NENA Master Glossary)
A database of street names and house number ranges within their associated communities defining Emergency Service Zones (ESZs) and their associated Emergency Service Numbers (ESNs) to enable proper routing of 9-1-1 calls.

Megabits/second (Mbps)
A measure of data transfer rates equal to one thousand kilobits or one million bits per second.

Megahertz (MHz) (NTFI Guide – Glossary of Terms)
A unit of frequency denoting one million Hz.

Memorandum of Understanding (MOU) (NTFI Guide – Glossary of Terms)
An agreement of cooperation between organizations defining the roles and responsibilities of each organization in relation to the other or others with respect to an issue over which the organizations have concurrent jurisdiction.

Mesh network
A communications network in which nodes connect to two or more other nodes. A node may be an end-user device, such as a computer, or a junction point between other pieces of the network. Mesh networks are used for redundancy, resiliency, and traffic balancing. They can be wired or wireless.

Metropolitan Area Network (MAN)
An organized collection of local area networks (LANs) across several locations in a municipal or metropolitan area connected by high-speed links to form a larger logical network.

Milestone (COPS Law Enforcement Tech Guide)
A significant event in the project, usually completion of a major deliverable.

Mobile data computer (MDC)
A computer installed in a vehicle to provide users with data communications over a wireless network. The computer is part of a system in the vehicle, which typically also includes one or more software applications running on the computer and a radio to send and receive data. Analog radio systems also require a modem to convert data to and from audio transferred over the radio channel, while digital systems, commercial or agency-owned, pass data without conversion.

Mobile data terminal (MDT)
An early type of mobile computing device dedicated to displaying data received across a radio network and unable to run software applications. The term "MDT" is often used synonymously today as computers have replaced dumb terminals.

Mutual aid interoperability (FCC PSWAC Final Report)
This involves multiple agencies using radios in "on-the-scene" incidents that are often outside the range of fixed infrastructure. There is often little opportunity for prior planning of different agencies to coordinate the necessary talk groups and frequency assignments.

National Broadband Plan (NBP)
The NBP is a Federal Communications Commission (FCC) plan which deals with improving broadband Internet access throughout the United States, including public safety.

National Coordination Committee (NCC) (NTFI Guide – Glossary of Terms)
The NCC was established by the FCC to solicit input from the public safety community in the further development of rules governing the new 700 MHz public safety band, particularly in regard to interoperability.

National Emergency Communications Plan (NECP)
The NECP is a strategic plan that sets goals and identifies key national priorities to enhance governance, planning, technology, training and exercises, and disaster communications capabilities.

National Environmental Policy Act (NEPA)
This federal law enacted in 1969 applies to programs and projects licensed/permitted or funded, including grants in aid, by the federal government that might have a significant impact on the quality of the human environment. Major federal actions affecting the human environment require completion of an environmental impact statement (EIS) or possibly an environmental assessment (EA). Radio communications projects financed in whole or part by federal funds are often subject to NEPA, particularly if any building or tower construction is involved.

National Information Exchange Model (NIEM)
NIEM is a national effort—sponsored by the Federal Government but with involvement from state, local, tribal, and international government representatives—to provide a common vocabulary and set of tools that support information exchange among justice, public safety, homeland security, intelligence, health, and many other domains.

National Infrastructure Protection Plan (NIPP)
The NIPP provides a unifying framework that integrates a range of efforts designed to enhance the safety of our nation's critical infrastructure.

National Institute of Justice (NTFI Guide – Glossary of Terms)
NIJ is the research and development agency of the U.S. Department of Justice.

National Interoperability Baseline Survey
The *National Interoperability Baseline Survey* was designed to assess and generate insights into five critical areas that determine an organization's capacity for interoperability—governance through administration and decision-making, standard operating procedures, technology, training and exercises, and usage of interoperable communications.

National Preparedness Guidelines
The *Guidelines* define what it means for the nation to be prepared to respond to major events.

National Response Framework
The *Framework* establishes a comprehensive, national, all-hazards approach to domestic incident response.

National Task Force on Interoperability
The NTFI was created by NIJ in 2002. It consisted of 18 national associations representing state and local elected and appointed officials and public safety officials. Through NIJ, the Task Force produced *Why Can't We Talk? Working Together to Bridge the Communications Gap to Save Lives, A Guide for Public Officials*.

Network (FCC Glossary of Telecommunications Terms)
Any connection of two or more computers that enables them to communicate. Networks may include transmission devices, servers, cables, routers, and satellites. The phone network is the total infrastructure for transmitting phone messages.

Next Generation 9-1-1 (NG9-1-1)
NG9-1-1 refers to an initiative aimed at updating the 9-1-1 service infrastructure in the United States and Canada to improve public emergency communications services in a wireless mobile society.

Pager (NTFI Guide – Glossary of Terms)
A communications device in which the intended receiver is alerted to receive a message or return a call.

Paging system (FCC Glossary of Telecommunications Terms)
A one-way mobile radio service where a user carries a small, lightweight miniature radio receiver capable of responding to coded signals. These devices, called "pagers," emit an audible signal, vibrate, or do both when activated by an incoming message.

Patch (NTFI Guide – Glossary of Terms)
A control center subsystem that permits a mobile or portable radio on one channel to communicate with one or more radios on a different channel through the control center console.

Performance reports (COPS Law Enforcement Tech Guide)
Provides details about project status, including which deadlines have been met and which have not. Whether prepared by the vendor or internal staff, performance reports should be provided on a weekly or biweekly basis.

Performance testing (COPS Law Enforcement Tech Guide)
A type of acceptance testing that is designed to determine the speed of the combined hardware and software package during various transactions.

Personal Area Network (PAN)
A basic communications networking type used to describe voice and/or data networks used by public safety agencies for both routine operations and emergencies. A PAN is a short-range network for communications among computer and telecommunications devices in the immediate vicinity of one person.

Personal Communications Services (PCS)
(FCC Glossary of Telecommunications Terms)
Any of several types of wireless, voice, and/or data communications systems, typically incorporating digital technology. PCS licenses are most often used to provide services similar to advanced cellular mobile or paging services. However, PCS can also be used to provide other wireless communications services, including services that allow people to place and receive communications while away from their home or office, as well as wireless communications to homes, office buildings, and other fixed locations.

Project 25 (P25) Standards (NTFI Guide – Glossary of Terms)
A joint government/industry standards-setting effort to develop technical standards for the next generation of public safety radios, both voice and data.

Project 25 (P25) Compliance Assessment Program (CAP)
The intent of the program is to provide vendors with a way of testing their products and to ultimately help public safety officials make better purchasing decisions.

Project charter (COPS Law Enforcement Tech Guide)
A document developed early in the process (prior to the full project plan) that contains an IT project description, complete with scope, objectives, organization, and staffing, a decision-making structure, the project management approach, and initial resource documents. Provides guidance to project staff in planning and designing a system.

Project management (COPS Law Enforcement Tech Guide)
The application of knowledge, skills, tools, and techniques to project activities in order to move the project forward to completion and to meet or exceed stakeholder needs and expectations from a project.

Project manager (COPS Law Enforcement Tech Guide)
An individual dedicated to and accountable for all project-related activities and solely responsible for the project's scope, quality, and budget. Responsible for virtually all aspects of the initiative and is formally accountable to the steering committee and the executive sponsor.

Project objectives (COPS Law Enforcement Tech Guide)
Quantifiable criteria that must be met for the project to be considered successful. A critical part of scope, objectives must include measures of quality, time, cost, performance, reliability, and functionality.

Project planning (COPS Law Enforcement Tech Guide)
A dynamic process that results in a document that guides the entire IT project design, procurement, implementation, and future enhancements. The plan is the repository for all project-related research, decisions, deliverables, and documents.

Project scope (COPS Law Enforcement Tech Guide)
Clearly defines the boundaries for the project. Scope addresses what users want (functions); how well the user requirements are met (quality of); when and how it must be developed (constraints); and why (the value in the project).

Project timeline (COPS Law Enforcement Tech Guide)
A mechanism to ensure the project is accurately and realistically scheduled so that it can be completed on time within the resources available. The timeline is critical to help avoid delays and associated cost overruns. Includes activities, deliverables, and milestones.

Proprietary software (NTFI Guide – Glossary of Terms)
Signaling protocol or software that is unique to a manufacturer and incompatible with other manufactured systems.

Proprietary systems roaming
A means of interagency communications in which cooperating agencies using similar, but proprietary, systems are able to communicate with each other and use the extended geographic coverage afforded by neighboring systems.

Protocol (NTFI Guide – Glossary of Terms)
A set of unique rules specifying a sequence of actions necessary to perform a communications function.

Public safety service providers (NTFI Guide – Glossary of Terms)
Persons who perform emergency first response missions to protect and preserve life, property, and natural resources and to serve the public welfare through federal, state, or local governments as prescribed by law. Public safety service providers also include non-governmental organizations that perform public safety functions on behalf of the government. For example, a number of local governments contract with private groups for emergency medical services.

Public safety support providers (NTFI Guide – Glossary of Terms)
Includes those whose primary mission might not fall within the classic public safety definition, but whose mission may provide vital support to the general public and/or the public safety official. Law enforcement, fire, and EMS would fit the first category, while transportation or public utility workers would fit the second.

Public Safety Wireless Advisory Committee (PSWAC) (NTFI Guide – Glossary of Terms)
A joint advisory committee of the FCC and NTIA that provided recommendations on the specific wireless communications requirements of public safety agencies through 2010.

Public-private partnership (NTFI Guide – Glossary of Terms)
A partnering between public and private entities in developing and constructing a system or a building project. In the case of a statewide communications infrastructure, a state may enter into an agreement with a third party that will assume responsibility for communications coverage, capacity, growth, and interoperability. The state will pay an access fee for use and services and share in revenues from additional users. The state will also be freed from the need for further appropriations, as well as cost savings on maintenance, upgrades, and training.

Quality assurances (QA) (COPS Law Enforcement Tech Guide)
Tests that ensure the vendor's hardware and software perform according to specification.

Radio cache (NTFI Guide – Glossary of Terms)
A portable or permanent storage facility for radios.

Radio channel (NTFI Guide – Glossary of Terms)
An assigned band of frequencies sufficient for radio communication. Note 1: The bandwidth of a radio channel depends upon the type of transmission and the frequency tolerance. Note 2: A channel is usually assigned for a specified radio service to be provided by a specified transmitter.

Radio communications (NTFI Guide – Glossary of Terms)
Telecommunication by means of radio waves.

Radio equipment (NTFI Guide – Glossary of Terms)
As defined in Federal Information Management Regulations, any equipment or interconnected system or subsystem of equipment (both transmission and reception) that is used to communicate over a distance by modulating and radiating electromagnetic waves in space without an artificial guide. This does not include such items as microwave, satellite, or cellular telephone equipment.

Radio Frequency (RF) (NTFI Guide – Glossary of Terms)
Any frequency within the electromagnetic spectrum normally associated with radio wave propagation.

Recurring costs (COPS Law Enforcement Tech Guide)
Continuing costs that must be considered to support, maintain, and enhance hardware and software and user skills. Determine in concert with initial costs (defined above).

Risk management (COPS Law Enforcement Tech Guide)
A planning process that prepares the agency for dealing with potentially harmful events that could happen in a technology initiative. The risk management plan is prepared by the project manager and steering, user, and technical committees.

Satellite (FCC Glossary of Telecommunications Terms)
A radio relay station that orbits the earth. A complete satellite communications system also includes earth stations that communicate with each other via the satellite. The satellite receives a signal transmitted by an originating earth station and retransmits that signal to the destination earth station(s).

Scanner (FCC Glossary of Telecommunications Terms)
A radio receiver that moves across a wide range of radio frequencies and allows audiences to listen to any of the frequencies.

Schedule management plan (COPS Law Enforcement Tech Guide)
Provides a structured process for documenting, analyzing, and approving changes in the project schedule. The schedule management plan should be a formal process that is documented in the project plan.

Scope management plan (COPS Law Enforcement Tech Guide)
Provides a structured process for documenting, analyzing, and approving changes in project scope. The scope management plan should be a formal process that is documented in the project plan.

Scope planning (COPS Law Enforcement Tech Guide)
A process to precisely define and document specific activities and deliverables for a particular project. Clarifies and defines the project focus and keeps activities in control and within agreed-upon boundaries. Establishes a formal process for proactively managing changes in project scope.

Scope statement (COPS Law Enforcement Tech Guide)
Defines what is to be included in the project, as well as what is to be excluded. Developed by the project manager and user committee.

Scope-time-cost relationship (COPS Law Enforcement Tech Guide)
The project elements of scope, time, and cost are inextricably linked and have a proportional relationship. Should any one of these elements grow or reduce, the other two elements grow or reduce proportionally.

Service provider (FCC Glossary of Telecommunications Terms)
A telecommunications provider that owns circuit-switching equipment.

Shared channels
One of several means of achieving technical interoperability in which cooperating agencies designate specific, often dedicated, radio channels for interagency use. Most public safety radio bands have designated shared frequencies that are often used, though the term applies generally to any channels adopted for interagency communications.

Shared system (NTFI Guide – Glossary of Terms)
A communications system developed by two or more different entities (e.g., local and state law enforcement agencies) to share the effort of system development, maintenance, and operations. Benefits of shared systems include lower costs, widespread interoperability, community interaction, and shared management and control.

Signal (NTFI Guide – Glossary of Terms)
The detectable transmitted energy that carries information from a transmitter to a receiver.

Sole-source (COPS Law Enforcement Tech Guide)
A procurement tool used when an agency can show that the chosen vendor is the only vendor capable of supplying the required hardware, software, and services in the best interest of the agency.

Spectrum (NTFI Guide – Glossary of Terms)
The usable radio frequencies in the electromagnetic distribution. Specific frequencies have been allocated to the public safety community.

Stakeholders (COPS Law Enforcement Tech Guide)
Individuals and organizations who are actively involved in the project, or whose interests may be positively or negatively affected as a result of project execution or successful project completion.

Standards-based shared system
One of several means of achieving technical interoperability in which a radio system based on open standards serves multiple agencies.

Statement of Work (SOW) (COPS Law Enforcement Tech Guide)
Included as an exhibit in a contract, the SOW defines each task involved in the entire project. It is the blueprint for implementation.

Statewide Interoperability Coordinator (SWIC)
The SWIC serves as the cornerstone of the State's interoperability effort. The Coordinator's role is one of program management.

Statewide Communications Interoperability Plan (SCIP)
The Statewide Communications Interoperability Plan (SCIP) is a multijurisdictional and multidisciplinary statewide strategic plan to enhance emergency communications.

Steering committee (COPS Law Enforcement Tech Guide)
Members are generally high-level managers and/or supervisors within the agency. This group will ensure that a structured project management process is adopted and followed. Provides constant guidance and oversight to the project, its progress and deliverables, and will make most decisions related to the project.

SWOT (COPS Law Enforcement Tech Guide)
An acronym sometimes used in referring to a situation assessment, SWOT stands for Strengths, Weaknesses, Opportunities, Threats (see *Environmental Scan*).

System (NTFI Guide – Glossary of Terms)
Any organized assembly of resources and procedures united and regulated by interaction of interdependence to accomplish a set of specific functions.

Systems development lifecycle (SDLC) (COPS Law Enforcement Tech Guide)
A cyclical process regarding IT, with several stages, including planning, procurement, implementation, and management.

TCP/IP
See *Transmission Control Protocol and Internet Protocol.*

Task force interoperability (FCC PSWAC Final Report)
This involves federal, state, and/or local agencies using portable and/or covert radios, requiring extensive close-range communications, and roaming in and out of infrastructure coverage. Normally, prior planning opportunity exists.

Technical committee (COPS Law Enforcement Tech Guide)
Includes technical staff from the agency, as well as others from the agency's parent organization (e.g., city, county, or state), if such support is provided. This committee's role is to analyze the agency's existing technical environment and to research and propose solutions to the agency's business needs and problems.

Technology baseline report (COPS Law Enforcement Tech Guide)
A report that documents an organization's current technology environment. Created by the project manager with assistance from the technical committee, it is used to show how the current technology is used, as well as to determine how new technology could improve efficiency. The technology baseline report is also used in the procurement process.

Telecommunications Industry Association (TIA)
TIA is a nonprofit trade association that has produced a number of networking standards.

Telephony (FCC Glossary of Telecommunications Terms)
The word used to describe the science of transmitting voice over a telecommunications network.

Total Cost of Ownership (TCO) (COPS Law Enforcement Tech Guide)
Used in budget planning, TCO refers to the total costs associated with ownership, usage, and maintenance of the system over time.

Transmission Control Protocol (TCP)
Part of the Internet Protocol suite responsible for ensuring data packets are sent, received, and reassembled in the correct order for the appropriate application using the data. See also *Internet Protocol*.

Trunked radio system (NTFI Guide – Glossary of Terms)
A system that integrates multiple channel pairs into a single system. When a user wants to transmit a message, the trunked system automatically selects a currently unused channel pair and assigns it to the user, decreasing the probability of having to wait for a free channel for a given channel loading.

Universal Mobile Telecommunications System (UMTS)
A wideband CDMA technology for mobile digital telephony and data intended as the successor for GSM networks. It promises data rates approaching 2 Mbps. Also known as 3GSM.

User committee (COPS Law Enforcement Tech Guide)
Includes subject matter and business process experts for the functions to be addressed. This committee's role is to assist and support in creating a project charter and ultimately the project plan. This committee will analyze existing workflows, define business processes, look for efficiencies, and establish the requirements of any new system.

Very High Frequency (VHF) (FCC Glossary of Telecommunications Terms)
The part of the radio spectrum from 30 to 300 megahertz, which includes TV Channels 2-13, the FM broadcast band and some marine, aviation, and land mobile services.

Vision statement (COPS Law Enforcement Tech Guide)
Written by the steering committee, the vision brings a tangible reality to what the agency will address with the new system.

Voice over Internet Protocol (VoIP)
A protocol for voice telephony over common data networks.

Wide Area Network (WAN)
A telecommunications network connecting separate local area networks and individual users. The Internet is considered a wide area network.

Wide Integrated Digital Enhanced Network (WiDEN)
An enhanced version of iDEN combining four standard channels to create 100 kHz radio channels for moderate speed data communications. Considered to be a 2.5G wireless service. iDEN™ is a trademark of Motorola, Inc.

Wi-Fi
The interoperable standard for IEEE 802.11 wireless local area network implementations. Conformance testing is carried out by the Wi-Fi Alliance, an industry group. Wi-Fi® is a registered trademark of the Wi-Fi Alliance.

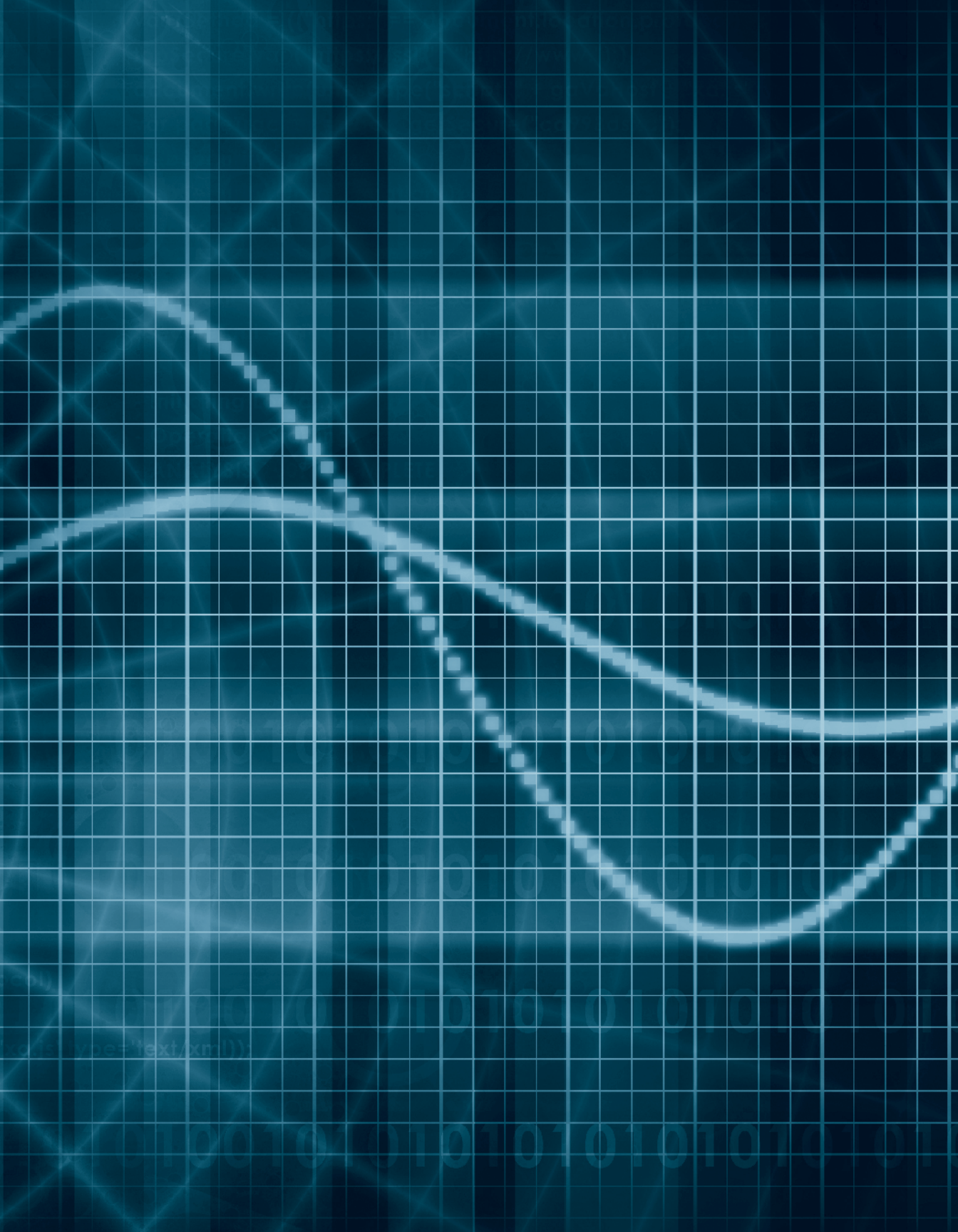
WiMAX
The interoperable standard for IEEE 802.16 wireless metropolitan area network (MAN) implementations. Conformance testing is carried out by the WiMAX Forum, an industry group.

Wireless LAN (WLAN) (NTFI Guide – Glossary of Terms)
A local area network that uses radio frequency technology to transmit network messages through the air for relatively short distances, such as across an office building or college campus. A wireless LAN can serve as a replacement for or extension to a wired LAN.

Work breakdown structure (WBS) (COPS Law Enforcement Tech Guide)
A component of the scope statement. Dissecting scope by breaking it down into smaller elements or projects produces specific deliverables and indicates who is responsible for enacting them. This ultimately defines activities and milestones of the full project scope.

XML (World Wide Web Consortium – W3C)
Extensible Markup Language. A simple, very flexible text format derived from SGML (ISO 8879). Originally designed to meet the challenges of large-scale electronic publishing, XML is also playing an increasingly important role in the exchange of a wide variety of data on the web and elsewhere.

Appendix G: SAFECOM Interoperability Continuum



Appendix G:
SAFECOM Interoperability Continuum

The following is provided by the U.S. Department of Homeland Security (DHS), Science and Technology Directorate's Office for Interoperability and Compatibility's SAFECOM Program.

Interoperability Continuum: A tool for improving public safety communications and interoperability.

Overview

The *Interoperability Continuum* is designed to help the public safety community and local, tribal, state, and federal policy makers address critical elements for success as they plan and implement interoperability solutions. The five elements of the continuum are:

1. Governance
2. Standard operating procedures (SOPs)
3. Technology (voice and data)
4. Training and exercises
5. Frequency of use of interoperable communications

The *Interoperability Continuum* was developed in accordance with the SAFECOM Program's locally driven philosophy and its practical experience in working with local governments across the nation. This tool was established to depict the core facets of interoperability according to the stated needs and challenges of the public safety community and will aid public safety practitioners and policy makers in their short- and long-term interoperability efforts.

Communications interoperability refers to the ability of public safety agencies to talk across disciplines and jurisdictions via radio communications systems, exchanging voice and/or data with one another on demand, in real time, when needed, and as authorized.

Making progress in all aspects of interoperability is essential, since the elements are interdependent. Therefore, to gain a true picture of a region's interoperability, progress along all five elements of the continuum must be considered together. For example, when a region procures new equipment, that region should plan training and conduct exercises to make the best use of that equipment.

To drive progress along the five elements of the continuum and improve interoperability, public safety practitioners should observe the following principles:

- Gain leadership commitment from all disciplines (Emergency Medical Services (EMS), Fire, Law Enforcement)
- Foster collaboration across disciplines through leadership support
- Interface with policy makers to gain leadership commitment and resource support
- Use interoperability solutions on a regular basis
- Plan and budget for ongoing updates to systems, procedures, and documentation
- Ensure collaboration and coordination across all elements (Governance, SOPs, Technology, Training/ Exercises, Usage)

Leadership, Planning, and Collaboration

In addition to progression along the five elements of the *Interoperability Continuum*, regions should focus on planning, conducting education and outreach programs, and maintaining an awareness of the specific issues and barriers that affect a particular region's movement toward increased interoperability. For example, many regions face difficulties related to political issues and the relationships within and across emergency response disciplines (e.g., EMS, fire-rescue response, and law enforcement) and jurisdictions. Leaders of all agencies and political subdivisions should help to work through these challenging internal and jurisdictional conflicts as well as set the stage for a region's commitment to the interoperability effort. Additionally, leaders must be willing to commit the time and resources necessary to ensure the sustained success of any interoperability effort. For example, ongoing maintenance and support of the system must be planned and incorporated into the budget.

In addition, collaboration should involve other agencies and organizations that may be critical in supporting the mission of emergency responders. Examples include emergency management agencies, the National Guard, public works, educational institutions/schools, transportation, medical facilities, and large private facilities.

Sustainability

Communications interoperability is an ongoing process, not a one-time investment. Once a governing body is set up, it must be prepared to meet on a regular basis, drawing on operational and technical expertise to plan and budget for continual updates to systems, procedures, and training and exercise programs. If regions expect emergency responders to use interoperable equipment on a daily basis, supporting documentation and the installed technology must be well-maintained with a long-term commitment to upgrades and the eventual replacement of equipment.

Lastly, an interoperability program should include both short- and long-term solutions. Early successes can help motivate regions to tackle more time-consuming and difficult challenges. It is critical, however, that short-term solutions do not inappropriately drive the planning process, but function in support of a long-term plan.

National Frameworks

As an evolving tool, the *Interoperability Continuum* supports the National Preparedness Strategy and aligns with national frameworks including, but not limited to, the National Response Framework, the National Incident Management System, the National Emergency Communications Plan, and the National Communications Baseline Survey. To maximize the Interoperability Continuum's value to the emergency response community, SAFECOM will regularly update the tool through a consensus process involving practitioners, technical experts, and representatives from local, tribal, state, and federal agencies.

Interoperability Continuum Elements

Governance

Establishing a common governing structure for solving interoperability issues will improve the policies, processes, and procedures of any major project by enhancing communication, coordination, and cooperation; establishing guidelines and principles; and reducing any internal jurisdictional conflicts. Governance structures provide the framework in which stakeholders can collaborate and make decisions that represent a common objective. It has become increasingly clear to the emergency response community that communications interoperability cannot be solved by any one entity; achieving interoperability requires a partnership among emergency response organizations across all levels of government. As such, a governing body should consist of local, tribal, state, and federal entities as well as representatives from all pertinent emergency response disciplines within an identified region.

Individual Agencies Working Independently – A lack of coordination among responding organizations.

Informal Coordination Between Agencies – Loose line-level or agency-level agreements that provide minimal incident interoperability.

Key Multi-Discipline Staff Collaboration on a Regular Basis – A number of agencies and disciplines working together in a local area to promote interoperability.

Regional Committee Working within a Statewide Communications Interoperability Plan Framework – Multidisciplinary jurisdictions working together across a region pursuant to formal written agreements as defined within the larger scope of a state plan—promoting optimal interoperability.

Standard Operating Procedures

Standard operating procedures—formal written guidelines or instructions for incident response—typically have both operational and technical components. Established SOPs enable emergency responders to successfully coordinate an incident response across disciplines and jurisdictions. Clear and effective SOPs are essential in the development and deployment of any interoperable communications solution.

Individual Agency SOPs – SOPs exist only within individual agencies and are not shared, resulting in uncoordinated procedures and/or incompatible data systems among agencies that can hinder effective multi-agency/multidiscipline response.

Joint SOPs for Planned Events – The development of SOPs for planned events. This typically represents the first phase as agencies begin to work together to develop interoperability.

Joint SOPs for Emergencies – SOPs for emergency-level response that are developed as agencies continue to promote interoperability.

Regional Set of Communications SOPs – Regionwide communications SOPs for multiagency/multidiscipline/multihazard responses serve as an integral step toward optimal interoperability.

National Incident Management System-Integrated SOPs – Regional SOPs are molded to conform to the elements of the National Incident Management System.

Technology

Technology is a critical tool for improving interoperability, but it is not the sole driver of an optimal solution. Successful implementation of data and voice communications technology is supported by strong governance and is highly dependent on effective collaboration and training among participating agencies and jurisdictions. Technologies should meet the needs of practitioners on the frontlines and should address regional needs, existing infrastructure, cost vs. benefit, and sustainability. The technologies described within the *Continuum* must be scalable in order to effectively support day-to-day incidents as well as large-scale disasters. Many times, a combination of technologies is necessary to provide effective communications among emergency responders. Security and authentication challenges are present in each technology and must be considered in all implementation decisions.

Data Elements

Swap Files – Swapping files involves the exchange of stand-alone data/application files or documents through physical or electronic media (e.g., universal serial bus devices, network drives, e-mails, faxes). This process effectively creates a static "snapshot" of information in a given time period. Though swapping files requires minimal planning and training, it can become difficult to manage beyond one-to-one sharing. With data frequently changing, there may be issues concerning the age and synchronization of information, timing of exchanges, and version control of documents. Each of these issues can hinder real-time collaborative efforts. In addition, the method of sharing files across unprotected networks raises security concerns.

Common Applications – The use of common proprietary applications requires agencies to purchase and use the same or compatible applications and a common vocabulary (e.g., time stamps) to share data. Common proprietary applications can increase access to information, improve user functionality, and permit real-time information sharing between agencies. However, the use of common proprietary applications requires strong governance to coordinate operations and maintenance among multiple independent agencies and users; these coordinated efforts are further compounded as the region expands and additional agencies use applications. Common proprietary applications also limit functionality choices as all participating agencies must use compatible applications.

Custom-Interfaced Applications – Custom-interfaced applications allow multiple agencies to link disparate proprietary applications using single, custom "one-off" links or a proprietary middleware application. As with common applications, this system can increase access to information, improve user functionality, and permit real-time information sharing among agencies. Improving upon common applications, this system allows agencies to choose their own application and control the functionality choices. However, if using one-to-one interfaces, the use of multiple applications requires custom-interfaces for each linked system. As the region grows and additional agencies participate, the required number of one-to-one links will grow significantly. Proprietary middleware applications allow for a more simplified regional expansion; however, all participants must invest in a single "one-off" link to the middleware, including any state or federal partners. Additionally, custom-interfaced applications typically require more expensive maintenance and upgrade costs. Changes to the functionality of linked systems often require changes to the interfaces as well.

One-Way Standards-Based Sharing – One-way standards-based sharing enables applications to "broadcast/push" or "receive/pull" information from disparate applications and data sources. This system enhances the real-time common operating picture and is established without direct access to the source data; this system can also support one-to-many relationships through standards-based middleware. However, because one-way standards-based sharing is not interactive, it does not support real-time collaboration between agencies..

Two-Way Standards-Based Sharing – Two-way standards-based sharing is the ideal solution for data interoperability. Using standards, this approach permits applications to share information from disparate applications and data sources and to process the information seamlessly. As with other solutions, a two-way approach can increase access to information, improve user functionality, and permit real-time collaborative information sharing between agencies. This form of sharing allows participating agencies to choose their own applications. Two-way standards-based sharing does not face the same problems as other solutions because it can support many-to-many relationships through standards-based middleware. Building on the attributes of other solutions, this system is most effective in establishing interoperability.

Voice Elements

Swap Radios – Swapping radios, or maintaining a cache of standby radios, is an age-old solution that is time-consuming, management-intensive, and likely to provide limited results due to channel availability

Gateway – Gateways retransmit across multiple frequency bands, providing an interim interoperability solution as agencies move toward shared systems. However, gateways are inefficient in that they require twice as much spectrum because each participating agency must use at least one channel in each band per common talk path, and because they are tailored for communications within the geographic coverage area common to all participating systems.

Shared Channels – Interoperability is promoted when agencies share a common frequency band, air interface (analog or digital), and are able to agree on common channels. However, the general frequency congestion that exists nationwide can place severe restrictions on the number of independent interoperability talk paths available in some bands.

Proprietary Shared Systems and Standards-based Shared Systems – Regional shared systems are the optimal solution to interoperability. While proprietary systems limit the user's choice of product with regard to manufacturer and competitive procurement, standards-based shared systems promote competitive procurement and a wide selection of products to meet specific user needs. With proper planning of the talk group architecture, interoperability is provided as a byproduct of system design, creating an optimal technology solution.

Training and Exercises

Implementing effective training and exercise programs to practice communications interoperability is essential for ensuring that the technology works and responders are able to effectively communicate during emergencies.

General Orientation on Equipment and Applications – Agencies provide initial orientation to their users with regard to their particular equipment and applications. Multiagency/multijurisdictional operations are often an afterthought to this training, if provided at all.

Single Agency Tabletop Exercises for Key Field and Support Staff – Structured tabletop exercises promote planning and identify response gaps. However, single agency activities do not promote interoperability across disciplines and jurisdictions. Additionally, management and supervisory training is critical to promoting routine use of interoperability mechanisms.

Multiagency Tabletop Exercises for Key Field and Support Staff – As agencies and disciplines begin working together to develop exercises and provide field training, workable interoperability solutions emerge. Tabletops should address data and/or voice communications interoperability and focus on effective information flow.

Multiagency Full Functional Exercises Involving All Staff – Once multiagency/multidiscipline plans are developed and practiced at the management and supervisory level, it is critical that all staff who would be involved in actual implementation receive training and participate in exercises.

Regular Comprehensive Region-wide Training and Exercises – Optimal interoperability involves equipment familiarization and an introduction to regional/state interoperability at time of hire (or in an academy setting). Success will be assured by regular, comprehensive, and realistic exercises that address potential problems in the region and involve the participation of all personnel.

Despite the best planning and technology preparations, there is always the risk of the unexpected—those critical and unprecedented incidents that require an expert at the helm who can immediately adapt to the situation. Within the Incident Command System, these specialists are called Communications Unit Leaders. The role of the Communications Unit Leader is a critical function that requires adequate training and cannot be delegated to an individual simply because that person "knows about communications systems." Rather, the proper training of these individuals is of significant importance to a region's ability to respond to unexpected events, and it should prepare them to manage the communications component of larger interoperability incidents by applying the available technical solutions to the specific operational environment of the event.

Usage

Usage refers to how often interoperable communications technologies are used. Success in this element is contingent upon progress and interplay among the other four elements on the *Interoperability Continuum*.

Planned Events – Events for which the date and time are known. (e.g., athletic events and large conferences/conventions that involve multiple responding agencies).

Localized Emergency Incidents – Emergency events that involve multiple intrajurisdictional responding agencies (e.g., a vehicle collision on an interstate highway).

Regional Incident Management – Routine coordination of responses across a region that include automatic aid fire response, as well as response to natural and manmade disasters.

Daily Use Throughout Region – Interoperability systems that are used every day for managing routine and emergency incidents. In this optimal solution, users are familiar with the operation of the system(s) and routinely work in concert with one another.

Building a voice or data communications system that allows police, fire, and emergency medical service agencies to communicate with each other within and across jurisdictions is a complex and costly effort. Revised and updated in 2012, the *Law Enforcement Tech Guide for Communications Interoperability* is a comprehensive, user-friendly guidebook that provides strategies, best practices, and recommendations for public safety agencies seeking to develop or expand interagency communications projects. It explores technologies in voice and data communications, and provides planning tools to help achieve interoperable communication initiatives. It serves as a companion to the COPS-funded *Law Enforcement Tech Guide: How to plan, purchase and manage technology (successfully!), A Guide for Executives, Managers and Technologists.*

U.S. Department of Justice
Office of Community Oriented Policing Services
145 N Street NE
Washington, DC 20530

To obtain details on COPS Office programs,
call the COPS Office Response Center at 800.421.6770.

Visit the COPS Office online at **www.cops.usdoj.gov**.

ISBN: 978-1-935676-55-3
e01124425
July 2013

Homeland Security

Interoperability Continuum

	Limited Leadership, Planning, and Collaboration Among Areas with Minimal Investment in the Sustainability of Systems and Documentation						High Degree of Leadership, Planning, and Collaboration Among Areas with Commitment to and Investment in Sustainability of Systems and Documentation
Governance		Individual Agencies Working Independently	Informal Coordination Between Agencies		Key Multi-Discipline Staff Collaboration on a Regular Basis	Regional Committee Working within a Statewide Communications Interoperability Plan Framework	
Standard Operating Procedures		Individual Agency SOPs	Joint SOPs for Planned Events	Joint SOPs for Emergencies	Regional Set of Communications SOPs	National Incident Management System Integrated SOPs	
Technology		***DATA ELEMENTS*** Swap Files ***VOICE ELEMENTS*** Swap Radios	Common Applications Gateway	Custom-Interfaced Applications Shared Channels	One-Way Standards-Based Sharing Proprietary Shared System	Two-Way Standards-Based Sharing Standards-Based Shared System	
Training & Exercises		General Orientation on Equipment and Applications	Single Agency Tabletop Exercises for Key Field and Support Staff	Multi-Agency Tabletop Exercises for Key Field and Support Staff	Multi-Agency Full Functional Exercises Involving All Staff	Regular Comprehensive Regionwide Training and Exercises	
Usage		Planned Events	Localized Emergency Incidents		Regional Incident Management	Daily Use Throughout Region	