Emergency Communications System Life Cycle Planning Guide

August 2011

Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528

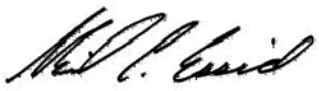
Dear Colleague:

Public safety systems, whether they are land mobile radio systems or mobile data systems, can be complex and costly to implement. There are many technical challenges, but it is also important that those entrusted to make decisions understand the elements that go into deploying and managing these systems. System life cycle planning is a critical part of this understanding because it enables practitioners to better forecast long-term funding requirements and helps to set the framework for establishing and maintaining a public safety system.

The Department of Homeland Security's Office of Emergency Communications within the National Protection and Programs Directorate's Office of Cybersecurity and Communications developed, with practitioner input, this System Life Cycle Planning Guide to assist you in your efforts to design, implement, support, and maintain a public safety communications system. The guide walks you through a number of steps and provides a high-level description of each area to help you fully engage in successful systems life cycle management.

The guide is a starting point from which your organization can begin to plan and budget for a public safety system's implementation. Additionally, the guide provides information to help you educate agency or jurisdictional leadership on the complexity of public safety systems in support of your system justification.

I trust that you will find this guide helpful and encourage you to visit http://www.safecomprogram.gov to learn about numerous other resources available.



Chris Essid
Director

TABLE OF CONTENTS

1. DEFINITIONS

Sources: Many of the terms listed below were taken from one of the following three sources. As applicable, the source is indicated in parenthesis following the term:

- Community Oriented Policing Services (COPS) Office – *Law Enforcement Tech Guide: How to plan, purchase and manage technology (successfully!)*, 2002. (http://www.search.org/files/pdf/TECHGUIDE.pdf)
- COPS Office – *Law Enforcement Tech Guide for Communications Interoperability: A Guide for Interagency Communications Projects*, 2006. (http://www.search.org/files/pdf/CommInteropTechGuide.pdf)
- Department of Homeland Security Office of Emergency Communications – *National Emergency Communications Plan*, 2008.

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 of 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.

Chief Information Officer (CIO) / Chief Technical Officer (CTO)
The most senior management in the agency/organization with the responsibility for oversight of the information technology systems.

Contract (COPS Law Enforcement Tech Guide)
A binding agreement between an agency and a chosen vendor that defines the obligations between the parties, including deliverables, services, and responsibilities.

Executive committee
A Committee comprising senior executives and /or management chartered to further the goals of the organization and to make decisions relevant to the direction of the system or project.

Functional requirements document (FRD)

A formal document that includes the statement of "what the system is intended to do" versus "how it is supposed to do it." The document contains **all** of the salient requirements for the system and is often used to support the procurement process.

Funding streams (COPS Law Enforcement Tech Guide)

The variety of means by which an agency may obtain funding for a project, including internal budgets, state and Federal grant programs, bond measures, etc.

Gateway (COPS Law Enforcement Interop Guide)

In general telecommunications, a device that connects two or more different networks.

Interoperability (COPS Law Enforcement Interop Guide)

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.

Invitation to bid (ITB) (COPS Law Enforcement Tech Guide)

A procurement tool used to define an agency's requirements, contractual terms, and pricing mandates. Used rarely, an ITB requires a vendor either to accept all or none of the terms.

Life-cycle costing methods (COPS Law Enforcement Tech Guide)

Methods to determine the total cost of owning the technology, from procurement through upgrade and/or replacement.

National Emergency Communications Plan (NECP) (Office of Emergency Communications)

A plan designed to address gaps and determine solutions so that emergency response personnel at all levels of government and across all disciplines can communicate as needed, on demand, and as authorized. The NECP is the Nation's first strategic plan to improve emergency response communications and complements overarching homeland security and emergency communications legislation, strategies, and initiatives.

Performance testing (COPS Law Enforcement Tech Guide)

A type of acceptance testing designed to determine the speed of a combined hardware and software package during various transactions.

Project manager (COPS Law Enforcement Tech Guide)

An individual dedicated to, and accountable for, all project-related activities and who is solely responsible for the project's scope, quality, and budget. The project manager is responsible for virtually all aspects of the initiative and is formally accountable to the steering committee and the executive sponsor.

Public safety system

A system designed specifically to public safety standards that provides communications and information services /applications—both mobile and fixed—to an emergency service workforce. Services /applications include the transmission of command functions to / from management as well as the communication of tactical capabilities.

Recurring cost (COPS Law Enforcement Tech Guide)

Costs that must be considered to support, maintain, and enhance hardware and software and user skills. Recurring costs are determined in concert with initial costs.

Request for proposals (RFP) (COPS Law Enforcement Tech Guide)

A procurement tool used to obtain actual hardware, software, and services proposals from vendors.

Sole-source (COPS Law Enforcement Tech Guide)

A procurement tool used when an agency can show that the chosen vendor is the only one capable of supplying the required hardware, software, or services in the best interest of the agency.

Stakeholders (COPS Law Enforcement Tech Guide)

Individuals and organizations actively involved in the project or whose interests may be positively or negatively affected as a result of project execution or successful project completion.

Standard operating procedure (SOP)

A document that outlines the expected actions for various scenarios, including normal day-to-day operations and emergency situations.

Steering committee (COPS Law Enforcement Tech Guide)

A group generally consisting of high-level managers and /or supervisors within the agency that provides constant guidelines for and oversight of the project, its progress, and deliverables and makes most decisions related to the project. This group ensures that a structured project-management process is adopted and followed.

System planning team

A working group consisting of a team leader responsible for coordinating the activities of the team, which is composed of functional and technical representatives of the organization.

System sponsor

Usually the agency with the funding authority for the system.

Technical Committee (COPS Law Enforcement Tech Guide)

A group that analyzes the agency's existing technical environment and researches and proposes solutions to the agency's business needs and problems. The Technical Committee 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.

User Committee (COPS Law Enforcement Tech Guide)

A group that assists and supports the creation of a project charter and, ultimately, the project plan. The User Committee includes subject-matter and business-process experts for the functions to be addressed. This committee analyzes existing workflows, defines business processes, looks for efficiencies, and establishes the requirements of any new system.

Vision statement (COPS Law Enforcement Tech Guide)

A statement written by the Steering Committee that brings a tangible reality to what the agency will address with the new system.

2. INTRODUCTION

The Department of Homeland Security's (DHS's) Office of Emergency Communications (OEC) within the National Protection and Programs Directorate's Office of Cybersecurity and Communications supports and promotes the ability of emergency responders and government officials to continue to communicate in the event of natural disasters, acts of terrorism, and other man-made disasters and works to ensure, accelerate, and attain operable and interoperable emergency communications nationwide. The National Emergency Communications Plan (NECP) is a strategic plan to improve interoperability, operability, and continuity of communications for Federal, State, local, tribal, and territorial emergency responders. It was developed with input from all major national associations, Federal agencies, and the private sector, and established three goals that set key performance targets, seven objectives that focus priorities, and 92 milestones to track progress and keep implementation on schedule. NECP initiative 6.1 states that OEC will "conduct system life cycle planning to better forecast long-term requirements." This life cycle planning document to support long-term cost planning and budgeting addresses NECP Initiative 6.1.

The guide is intended to be a high-level review of the considerations relevant to each step of the system life cycle and is based on a Technology Life-cycle Management (TLM) model. The System Life Cycle Planning Guide takes into consideration existing relevant emergency communications life cycle planning documents as well as industry best practices for life cycle planning methodologies, such as Closed Loop Life-cycle Planning, System Development Life-cycle, and TLM. The guide is structured around the "Step" concept depicted in the system life cycle planning model in Figure 1 and provides a high-level overview of system life cycle management concepts.

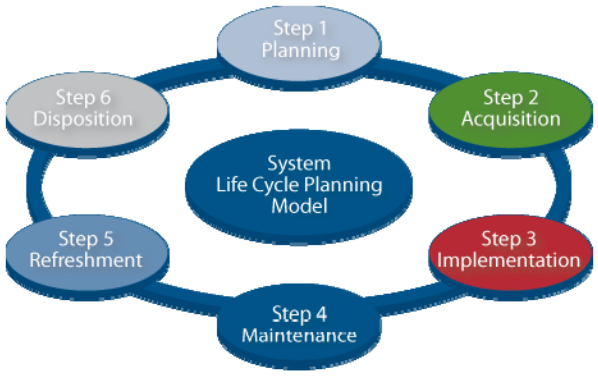


Figure 1 - System Life Cycle Planning Model

3. SYSTEM LIFE CYCLE MANAGEMENT

Step 1 - PLANNING

Goal: *To establish a formal planning team, identify all key elements of the impacted system, and document the operational and technical requirements to support system replacement or upgrade.*

Timing: *Twelve to 18 months before system replacement or upgrade*

In This Step: *Establish a planning team;*
Identify the purpose, goals, and timelines for the impacted system;
Define functional and technical requirements; and
Document the requirements in a Functional Requirements Document (FRD)

Key Stakeholders: *Executive and Middle Management (Chief/Director), End Users, and Technical Staff*

Key Deliverables: *The FRD*

Consider: *System planning is not strategic planning; however, it can be the outcome of a strategy. System planning occurs after a strategic decision has been made to replace, upgrade, maintain, dispose of, or acquire a system. For more information on strategic plans, please review,* Roadmap for Integrated Justice: A Guide for Planning and Management (*http://www.search.org/files/pdf/StrategicRoadmap.pdf), which provides an overview of strategic planning.*

1. SYSTEMS PLANNING TEAM

Is it time to start? Setting a firm foundation is a key to building a good plan. Having the right players involved will help make sure the system planning process is sound, inclusive, and finishes with a high degree of success. Get a good team structure in place now; the time to work will follow.

1.1. GOVERNANCE

Sponsorship – It is essential for any successful public venture to have full sponsorship from the highest-possible management level and complete buy-in from all relevant stakeholders. Systems that support a geographically dispersed circle of supported agencies will require authorization from higher, and often political, levels.

Representation – Public safety systems encompass a diverse group of disciplines, such as law enforcement, fire, and emergency medical service (EMS); they must be representative of the agencies affected by the project and have full authorization to participate on behalf of the agencies they represent.

Participation – The planning team should consist of multiple combinations of key personnel from both the technical and operational areas. The planning team structure is represented in Figure 2 and should consist of the following:

- Executive or Steering Committee;
- User Committee;
- Technical Committee; and
- Ad Hoc Working Groups.

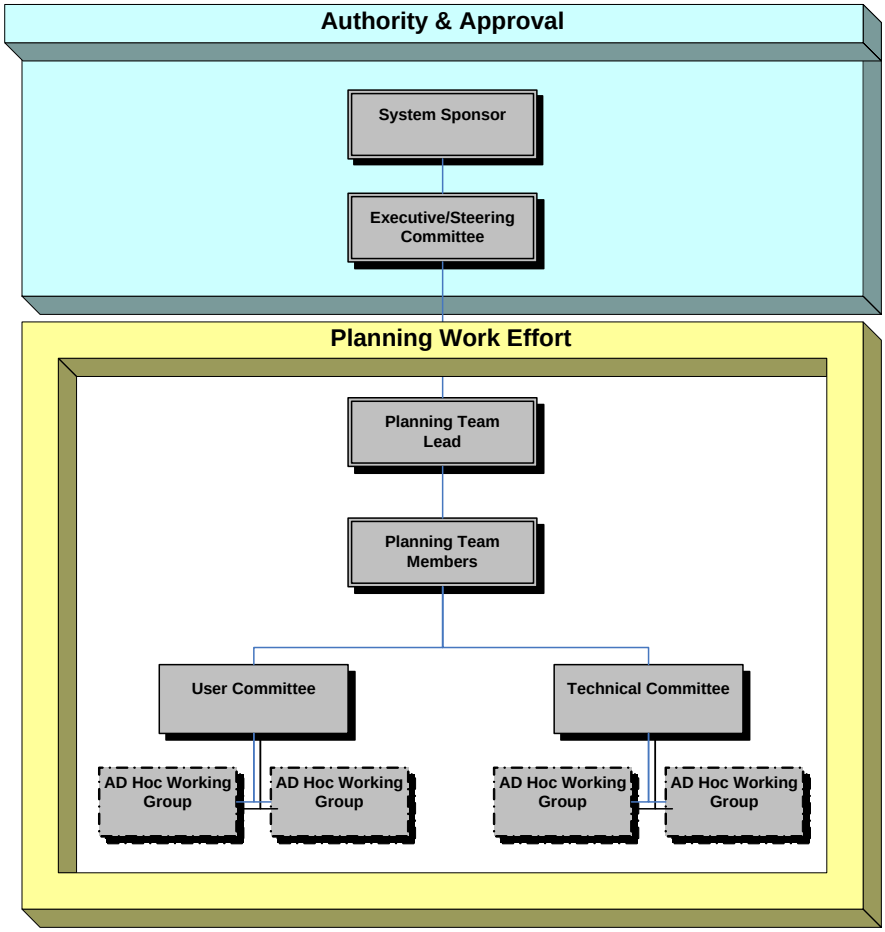


Figure 2 – System Life Cycle Planning Team[1]

1.2. PURPOSE

The planning team must have a comprehensive system charter that provides guidance to the team as they progress during the planning phase. Successful planning requires that the team members are on the same page and clearly understand the system scope, objectives, available resources, and decision-making structure.

[1] Modeled after Sample Project Decision-making Structure #1 found in Chapter 1, page 2 of the COPS Office's, *Law Enforcement Tech Guide: How to plan, purchase and manage technology (successfully!)* (http://www.search.org/files/pdf/TECHGUIDE.pdf).

1.3. GOALS

Establishing clear and concise goals is one of the planning team's first critical steps. The goals must be realistic and fully representative of the requirements of the representative agencies and/or departments.

1.4. TIMELINES

Timelines are a key to setting the stage for when systems need to be considered for replacement and implementation. Many factors in the public safety environment impact the planning team's assessment and delineation of key milestones. Key elements impacting timelines include:

- Institutional, legislative, and regulatory guidelines;
- Potential emergency situations, such as hurricanes and wildland fires;
- Budgeting cycles, grant benchmarks, data-collection requirements, report-generation steps, and authorization and review processes; and
- Manufacturer's expectation of the time during which the system will be operational—in other words, its "useful life." Vendors often refer to this as a vendor "roadmap" (Figure 3). It is important to pay special attention to when a system is scheduled for support and when its "end of life" occurs. These two factors affect decisions to upgrade/replace the system and also have a dramatic impact on the system timeline.

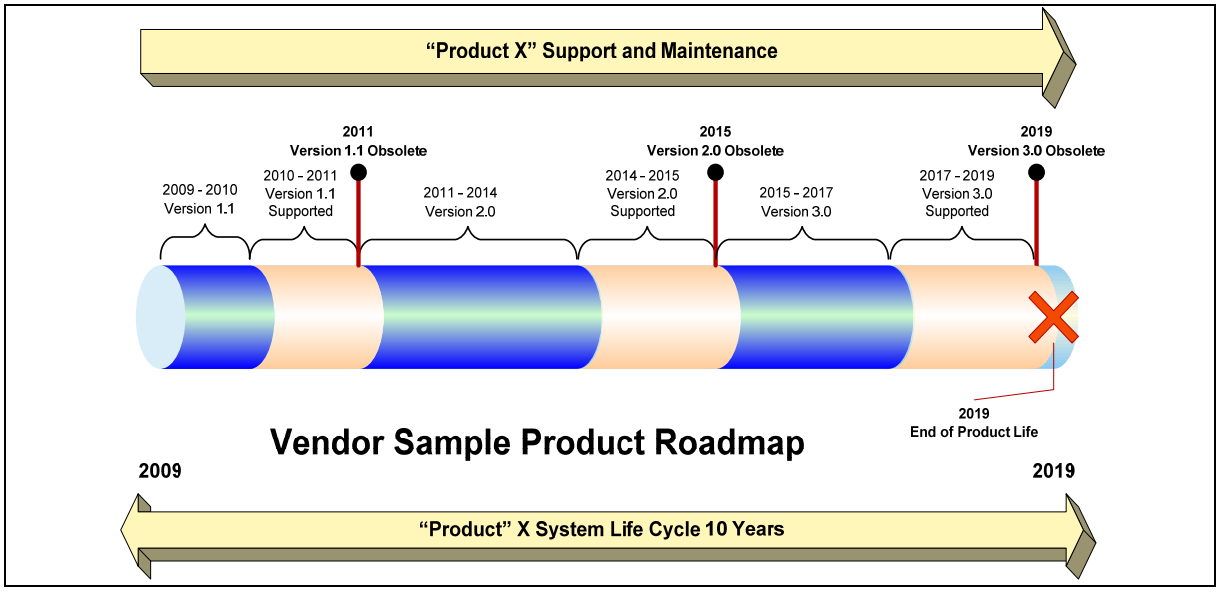


Figure 3 – Vendor Sample Product Roadmap

2. GATHERING FUNCTIONAL REQUIREMENTS

What does the system do or need to do? So, you have a team and it is time to get working – this phase will be the time to decide what the system will need to do for your agency. Gathering the operational and technical requirements takes work and significant interaction with stakeholders. Start gathering user input/feedback early and often to ensure that the new system meets your needs!

2.1. USER INPUT

Identify Key Stakeholders – Key stakeholders come from all areas of the organization and include:

- The Executive Sponsor, which may be the Chief Information Officer (CIO) / Chief Technical Officer (CTO), Public Safety Chief, or a representative of some other level of organizational management;
- Planning Team Lead, operational users, and technical staff; and
- External stakeholders, such as Federal, State, regional, and tribal partners, as well as local partners such as colleges and universities, hospitals, large corporations, and military installations.

Create the Business Case for System Replacement – Based on early input provided by key stakeholders, the case must be formulated for why the system is being considered for replacement. When building the business case, it is imperative to focus on the agency's ability to be operable and/or improve operability. If given the opportunity, it is also an ideal time to align with the various interoperability plans available for consideration:

- National Emergency Communications Plan (NECP) – http://www.dhs.gov/files/publications/gc_1217521334397.shtm;
- Statewide Communication Interoperability Plan (SCIP) – http://www.dhs.gov/files/programs/gc_1225902750156.shtm (or check with your State's interoperable communications program for access to your State SCIP);
- Regional Communications Interoperability Plan – Check with your regional governance groups;
- Tactical Interoperability Communications Plan – Check with your Urban Area Security Initiative governance committee; and
- Other relevant interoperability or communications plans as developed locally.

Get the Input – It is imperative to have a structured method for gathering user, technical, and functional requirements. Methods can include:

- Meetings – Depending on the size and scope of the project, these meetings may include a variety of agencies and/or departments;
- Interviews – For a system with a broad base of target users, it may be advantageous to hold individual agency/department interviews; and
- Surveys – A survey instrument may replace the need for direct meetings for smaller systems, and follow-up surveys will supply missing data for larger systems.

2.2. ALIGNING TECHNICAL REQUIREMENTS

Assess the Current Environment – Conduct an assessment of current inventory relevant to the system, to include:

- Operating systems, frequency identifications, licensing, and other applicable information;
- Support requirements, including maintenance, public/private facilities, and contracted services;
- Age and general amortization of the infrastructure along with expected remaining useful life; and
- Public entities that may be potential stakeholders in either using or supporting technology.

Additional Key System Considerations:

- Infrastructure – Identify the capacity of physical structures and their condition;
- Coverage – Document areas of known coverage problems and anticipated expansion of public areas;
- Subscriber Equipment – Inventory mobile/portable equipment, accessories, and channel loading;
- Peripheral Equipment – Inventory ancillary items such as gateways and interoperable equipment;
- Operational Standards – Consider operational standards and their impact on the system; and
- Future Trends – Collect un-served needs and anticipated upgrades.

2.3.INTEROPERABILITY REQUIREMENTS

Interoperability Continuum – Address the gaps in routine interaction (mutual aid) and emergency interaction (unplanned incidents) among adjacent agencies, jurisdictions, and disciplines. Document the interface and associations among the various stakeholders. These connections have a direct impact on the technology required to provide basic operational requirements. Become familiar with the concepts of interoperability as outlined in the DHSSAFECOM Interoperability Continuum (Figure 4). Technology will be an important facilitator toward reaching higher levels of interoperability.

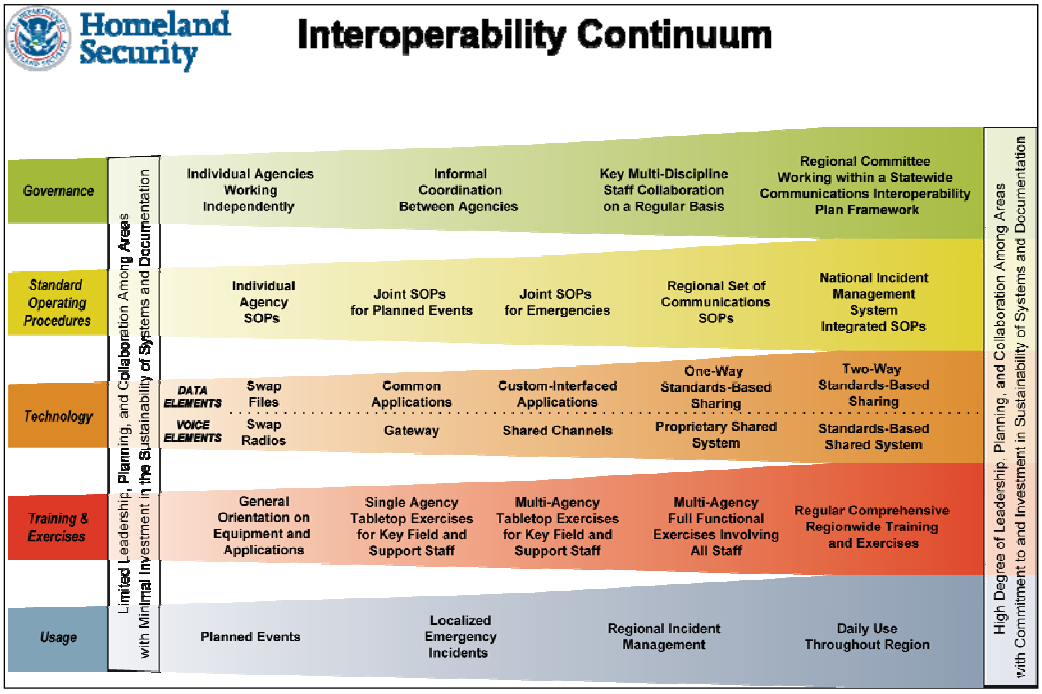


Figure 4 – DHS SAFECOM Interoperability Continuum

3. FUNCTIONAL REQUIREMENTS DOCUMENT

3.1. FUNCTIONAL REQUIREMENTS DOCUMENT DEVELOPMENT

Now what? You are done with gathering user requirements, and it is time to take all of the information and organize it into a concise document. Creating the Functional Requirements Document (FRD) is the next action in the Planning Step and helps set the foundation for Step 2 – Acquisition.

FRD – The FRD is developed based on the information acquired during the user requirement and technical requirement gathering outlined in Section 2. The current and future needs of participant agencies will be represented within the FRD. The FRD becomes a primary reference for any resulting procurement documents. Written with this purpose in mind, the FRD should be drafted in detail so that it could be dropped into a future procurement document with minimal alteration. The ultimate purpose of the FRD is to itemize the requirements clearly enough that potential future RFPs or other procurement instruments will allow prospective respondents to fully understand the scope and requirements of the system to provide an appropriate technical response.

What a FRD Should Contain – The FRD should include, at a minimum, the following sections:

- General Information – This section will address the background, purpose and scope of the system;
- Current System – This section will include the background, current system objectives, design, uses/methods, and limitations. It will also include a clear vision of the various agencies/departments participating in the system;
- Proposed Enhancements – This section will include improvements, impacts, and assumptions;
- System Design Details – This section will include performance requirements, capacity limitations, system description, system functionality, constraints, and backup needs. Descriptions and requirements should remain vendor neutral wherever possible;
- Environment – This section should address the system environment, including infrastructure, gateway/interfaces, subscriber, and software environment. Additional consideration should be given to operational impacts and dependencies, fail-over contingencies, and any other operational contingencies (e.g., training, overtime, staffing, maintenance, migration strategies, re-occurring costs, etc.); and
- Security – This section will include electronic and physical security considerations.

FRD Team – This is a group of key planning team members who are tasked with the following:

- Assembling and compiling information;
- Writing and editing the FRD; and
- Distributing the draft FRD document to the planning team for review and approval. (It is the responsibility of the planning team lead to obtain final approval from the Executive/Steering Committee.)

STEP 2 ACQUISITION

Goal: *The System Planning Team has done its job and delivered an FRD that now becomes the basis for the procurement. The goal now shifts to acquiring a new system.*

Timing: *Request for Proposal (RFP) Development – Six months after FRD Development*
Procurement Process – six to nine months after release of RFP

In This Step: *Create a budget for replacement;*
Identify the method of procurement – traditional large system procurements use RFP;
Assess purchasing options; and
Determine what elements to consider in a system purchase

Key Stakeholders: *Executive and Agency Middle Management (Chief/Director), Project Manager, and RFP Team (includes an agency's operational and technical staff), as well as the Purchasing, Legal, and Vendor Community*

Key Deliverables: *Procurement Document (RFP, Invitation to Bid, Sole Source, etc.) and System Contract*

Consider: *This is the time that the system planning process will transition to more traditional project planning requiring sound project management principles. For more information on project management methodologies, please review the COPS Office's* Law Enforcement Tech Guide: How to plan, purchase and manage technology (successfully!) *(http://www.search.org/files/pdf/TECHGUIDE.pdf).*

1. COMPONENTS OF A SYSTEM PURCHASE

What am I buying? A radio system is more than just a few towers and some radios, and those undefined items are the ones that add up. Make sure you clearly define all of the elements to help establish a budgetary estimate before you move to procurement.

1.1. BASIC SYSTEM COST ELEMENTS

Equipment – Communications systems have several discrete cost elements to consider.

Communication Sites – A basic radio system will require the placement of sites to house, transmit, receive, and control equipment. Site equipment can include:

- Transmit and Receive Equipment – Base stations, antennas, and control equipment;
- Control Equipment – Trunking controllers, system management terminals, etc.;
- Tower – Shelter, land improvements (fence, access), etc.; and
- Power – Primary and back-up power.

Backhaul Sites – Traditionally, these sites are collocated with communications sites—this is the network that is used to bring the radio signal back to the main/prime site. Backhaul can come in different modes, as follows:

- Leased Services – Commercial carriers can provide you with leased services for backhaul; and
- Agency/Jurisdiction Owned – There are two traditional methods for building out a backhaul system: wireless or wired.
    - Wireless – Based on microwave technology; provides a variety of throughput options;
    - Wired – Copper- or fiber-based; however, the industry is moving toward fiber because of its inherent survivability and higher transport speeds.

Subscriber – These are the devices deployed to field personnel and are traditionally the second most significant cost element of a system. Subscriber equipment can include:

- Portable and Mobile Radios – These are the radios normally deployed to field personnel. When considering radios, most vendors will have a variety of tiers. Also, mobile radios come with a variety of mounting and control head options and require installation and de-installation; and
- Additional Subscriber Radio Consideration – Obviously, the cost goes up as the tier level increases, so consider evaluating the different options and purchasing the radio that best fits rather than immediately jumping to a higher tier.

Consoles – Console or dispatch equipment must be installed for the dispatch center to communicate with the field personnel.

Peripheral Equipment – Other peripheral equipment supplementing the system can include:

- Remote base stations located in remote areas such as fire stations and other government facilities;
- Remote control consoles and handheld chargers; and

- Bi-directional amplifiers to ensure coverage inside buildings such as schools, large office buildings, malls, etc.

System Interfaces – Computer Aided Dispatch, Logging Recorders, Fire Station Alerting, etc.

Recurring Costs – Finally, there are recurring cost elements that must be considered:

- Ongoing infrastructure maintenance costs for software and hardware;
- Ongoing subscriber maintenance costs, including support, maintenance, and programming;
- Any site rental/lease fees;
- Backhaul connection services provided by commercial services, if applicable;
- Training, both initial training and ongoing regular training; and
- Technology refreshment, in the form of either regular system updates or retained funding for future upgrades.

1.2. INTEROPERABILITY COST CONSIDERATIONS

It appears as though incidents requiring multi-discipline and multi-jurisdictional response are a rising occurrence. Interdependencies of agencies of all types have become the norm. In designing systems, operability is certainly a key factor to consider; however, designing a system with interoperability in mind from the start becomes much more cost-effective than having to retrofit a system. The system that is designed with interoperability in mind is also much more efficient. Additionally, many Federal grant mechanisms require a specific reference to efforts incorporating interoperability in any supported projects. In the long run, interoperability will be a cost-savings effort considering the impact to the public and property.

1.3. OTHER SYSTEM COST IMPACTS

Software Costs – Include the cost of the software and any support cost for upgrades.

Warranties – Include the first year's warranty cost in the overall system investment. Assess the value of extended warranty offerings, as some vendors will offer discounts for bundling multiple-year warranties.

Replacement Cycles – Determine the support life for the system infrastructure and subscriber units.

Maintenance – Assess the various maintenance cost options. Review Step 4 for various alternatives.

Adjacent Agencies – Determine the impact of your system changes on adjoining agencies/departments.

Consolidation – Consider overlapping jurisdictions and any efforts at consolidation.

Training – Factor in sufficient training; modern systems are more sophisticated and require adherence to better, repeated user training.

Continuity of Operations – Consider the cost impact associated with the required level of systems redundancy.

2. FINANCIAL PLANNING

Can you afford it? Before you go through the process of buying a new system, it is best to spend some time up front to determine how much the system will cost and how you are going to pay for it. Once you have analyzed the data and have determined you can afford the system, it is time to move into procurement.

2.1. BUDGETING

A budgetary estimate follows the development of the basic cost elements of the system. As the COPS Law Enforcement Tech Guide series states: "Preparing the project budget is not rocket science… and requires only a few steps." The following steps are integral to preparing a budgetary estimate:

1. Gather Internal and External Cost Data;
2. Create a Project Budget of Initial Costs;
3. Estimate Recurring Costs and Include in Budget; and
4. Plan for Ongoing Updates to Project Budget.[2]

2.2. SOLICITATION, SELECTION, AND AWARD

Procurement – Moving forward requires a determination on the type of procurement. Three traditional methods exist:

- **Full and Open Competition - RFP:** A formal procurement document detailing the requirements of the new system; this method is best used on large system procurements awarded based on best value;
- **Full and Open Competition - ITB:** A formal procurement document best used to purchase a specific piece of equipment where installation is not required; not traditionally used for large radio or data systems; and

[2] Found in Chapter 11, page 138 of the COPS Office's *Law Enforcement Tech Guide: How to plan, purchase and manage technology (successfully!)* (http://www.search.org/files/pdf/TECHGUIDE.pdf).

- **Sole-source:** Contracting with one specific vendor without competition; this method should be used only as the last option and can raise the cost to the organization.

Award – Major systems should be awarded based on the best value for the procuring agency as defined by the offeror that best meets or exceeds all of the mandatory requirements and is the most experienced with the type of system. A word of caution: even the most technically sound system is only good if you can afford it.

Contract – Once an award is made, it is time to finalize the contract documents between the successful offeror and the awarding agency. The contract should include the following:

- All legal and financial responsibilities of both parties and the procurement document;
- The offeror's best and final offer, including relevant supporting documentation (e.g., propagation maps, project plan, acceptance test plans, etc.);
- Potential penalties for failure to perform; and
- Payment Terms tied to milestones (see sample payment milestone schedule in Figure 5 below).

Payment Milestone Description	% Paid
Completion of Customer Design Review	25%
Shipment of Radio Infrastructure Equipment	20%
Installation of Radio Infrastructure Equipment	25%
Initial Acceptance – Tied to ATP	10%
Final Acceptance – Tied to Final ATP	10%
Cutover – Operational For 90 Days	10%

Figure 5 – Sample Radio Infrastructure Milestone Payment Plan

2.3. PURCHASING OPTIONS

Purchases of public safety systems such as radio and mobile data systems usually require a substantial funding commitment on the part of the buying agency. Aside from yearly allocated general funds, several other options exist to cover procurement costs:

- **Capital Investment** – The magnitude of the expenditure, coupled with the product life cycle of 10 to 15 years, creates a situation where municipal planners need to begin to treat these systems similar to other infrastructure capital improvement projects related to roads, water and sewage, etc.

- **Grant Sources** – Many communications systems are taking advantage of Federal and State grant sources (see Anatomy of a Grant Program in Figure 6 below).

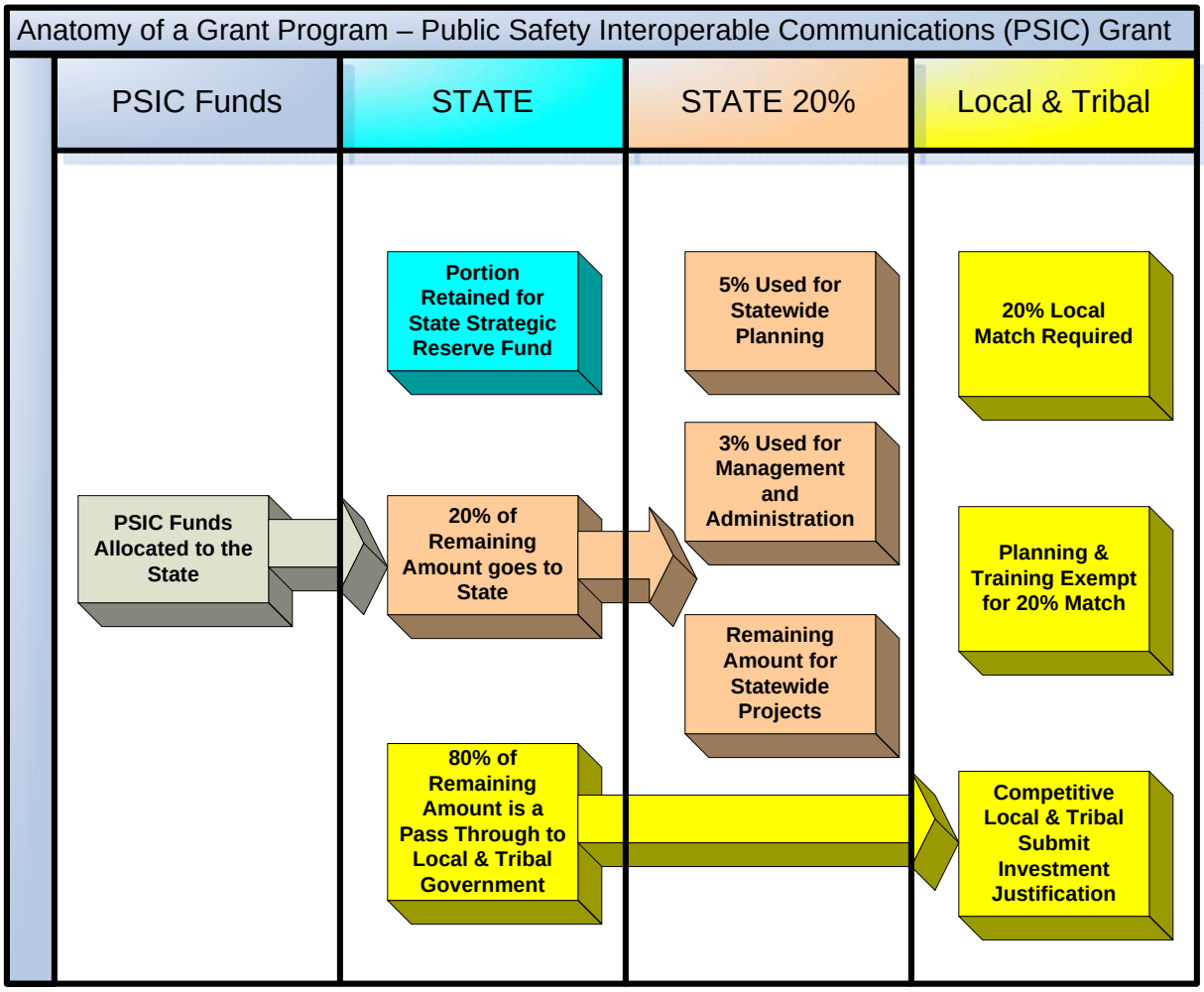


Figure 6 – Anatomy of a Grant Program

- **Vendor Options** – Vendors often are able to directly, or through associated investment partners, provide financial capabilities tailored to the needs of the agency(s).

- **Lease Purchase Option** – In conjunction with the vendor or other leasing agencies, consideration for leasing the system lessens the initial capital outlay and may accommodate local budgets.

2.4. SHARED SYSTEM CONSIDERATIONS

Reduce Total Cost of Ownership – The sophistication of many of the current advanced communications systems often comes at the price of high initial procurement costs as well as substantial ongoing operational overhead costs. Often this overhead and expense can be dispersed across many agencies. Newer systems that consider a regional approach have the advantage of lowering the total cost of ownership for the agency participants.

Cost savings can be realized by leveraging a shared system. In the example shown in Figure 7, a regional shared system approach can reduce potential tower sites from eight to as few as five.

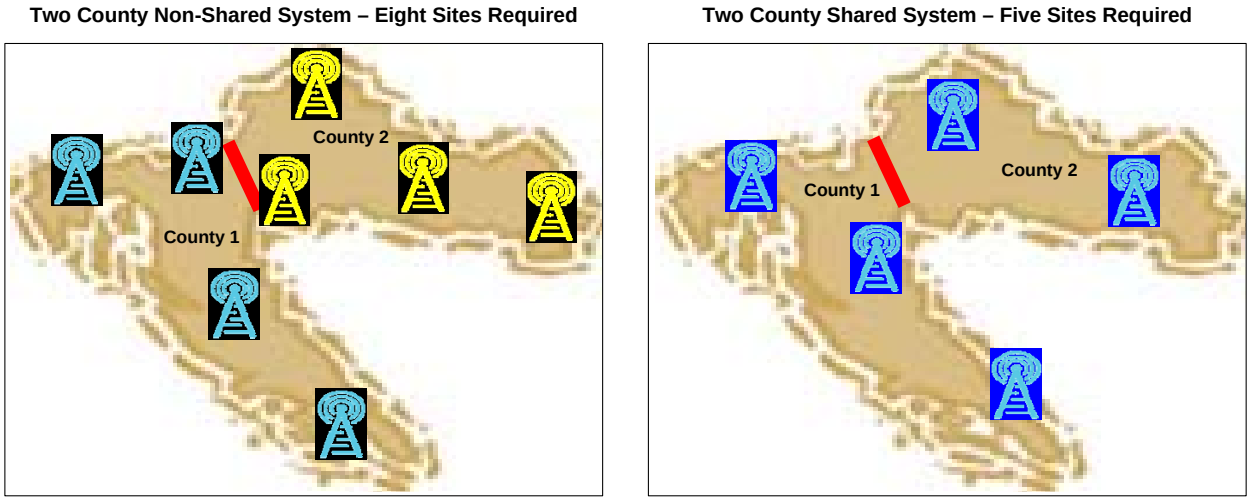


Figure 7 – Shared versus Non-Shared System

STEP 3 IMPLEMENTATION

Goal: *The System has been procured and will now be ordered, staged, installed, tested, and cutover. Once training is completed, the system will go live.*

Timing: *System Implementation – 12 to 18 months from contract award*

In This Step: *Create an implementation plan;*
Install new/upgraded system;
Test the system;
Train users; and
Go live

Key Stakeholders: *Project Manager, Implementation Team (includes an agency's operational and technical staff), Vendor Technical Staff, and End Users*

Key Deliverables: *Project Implementation Plan, Acceptance Test Plan, and Training Plan*

Consider: *User and agency buy-in have a large impact on the perceived success of the new system. Step 3 is a good time to consider implementing a communications plan to help market the impacts and benefits of the new system.*

1. STAGING

Does it work? Modern advanced communications systems are very complex and interdependent. The industry trend has been to "stage" these systems to validate initial system operation. This staging, however, still does not typically replicate a real world setting

1.1. STAGING

Factory Staging – This staging includes setting up the entire system at the vendor's factory location. This approach is good, but it does not reflect the real world.

On-Site Staging – This staging includes setting up the entire system at your location. This approach is better, but it still does not reflect the real world.

Cost is a consideration in both of the staging options. Traditionally, the vendor will pass on cost associated with staging to its customer. As such, an agency should try to determine the cost associated with each staging option, negotiate as appropriate, and incorporate staging to the extent practical.

2. INSTALLATION/INTEGRATION

Is it ready to use? All the work from Step 1 and 2 will now be realized as the system is put through the paces and any issues worked out to bring the new/upgraded system to full operational status.

2.1. TESTING/PROTOTYPING

The test procedures for verifying areas and level of coverage should be structured and tied to an acceptance test plan (ATP) that is fashioned from the FRD and technical specifications. Be sure your vendor and Technical Committee fully understand the testing criteria, testing procedures, and any dependencies (such as milestone payments, as depicted in Figure 5).

2.2. CUTOVER

Depending upon whether a new system is more of a moderate upgrade or a system overhaul, a cutover plan is necessary. Consider the following:

- Can you afford down time?
- How do you communicate if the prime system is down?
- Is there a better time of day to cut over during which incident volume is low?
- Do you have a tourist season to avoid? How about a hurricane season?
- Which should come first: subscribers or infrastructure?
- Do you have interoperability considerations (e.g., mutual aid, gateways, etc.?

2.3. GO LIVE

Reaching "Go Live" status on a new system is usually a transitional process. The process will consist of installation, testing of functionality, training, and correction of deficiencies. Once the system is cut over, the first 90 days are critical – this is when many of the problems will occur. Be sure to address all operator training requirements to avoid operator error. If possible, maintain your legacy system as a backup until you are confident the new system is fully capable.

2.4. INTEROPERABILITY IMPACTS

Inform and involve other agencies in your transition plans and identify any potential reduction in inter-department/agency communications; plan for alternate processes. Review your emergency communications plans to determine any impact ongoing operations will have on your regional interoperability capabilities.

The first step to interoperability is *operability*. Designing a system with interoperability in mind will minimize the cost and efforts involved. Planning with interoperability in mind is the best way to set an agency on the path to a robust response capability.

3. TRAINING

Do you know how to use it? The system is ready – are the users? Make sure you implement a training plan to include all users and support staff for the new/upgraded system. The technology side of the system tends to be the easy part; getting users to understand and use the technology is the hard part.

3.1. OPERATIONAL

Operational Personnel – All public first responders require extensive training to perform their primary mission. Emphasize any special requirements for interoperability communications as it relates to mutual aid.

Telecommunicator Personnel – Certain system features will be controlled by telecommunicator personnel through the radio dispatch system. Include these personnel in both initial and ongoing operational training.

Backup Procedures – Establishing backup procedures for potential system failures and providing related training is a must. Most systems have various means of alternate operation in the event of partial system failure or even total system failure. Include contingencies for interoperability.

3.2. TECHNICAL

Maintenance Personnel – The ongoing performance of any communications system will be directly related to its maintenance. Include requirements for training of internal or local personnel (if contracted) in the total system.

System Management – A new feature of modern systems is the requirement for "system management." Specialized training, available through the vendor, is required for those person(s) who will be charged with system management.

3.3. INTEROPERABILITY

Provide training for users on interoperability, focusing on any changes to existing procedures as the result of the new system. Discuss with other interoperability partners the changes and their affect on current mutual aid/interoperability procedures. Alter appropriate documents and plans. Organize post-implementation joint training to reinforce initial training and verify interoperability. Apply all "lanes" of the Interoperability Continuum.

4. SYSTEM ACCEPTANCE

It works, but do you keep it? It is now time to make the decision to accept the system. Formal testing tied to the original FRD established in Step 2 will make this step easy.

4.1. INITIAL ACCEPTANCE

Acceptance of a system will be highly dependent upon final performance; however, interim testing and evaluation should be conducted throughout the project to ensure that measured progress is being made toward system completion. An initial ATP should be developed and followed to ensure that formal testing is conducted.

4.2. FINAL ACCEPTANCE

Any resulting deficiencies from the initial acceptance test should now be resolved and tested. A final ATP (FATP) should be developed and followed to ensure formal acceptance. Positive completion of the FATP indicates that the system, as tested, performs to the requirements and specifications proposed. This does not mean that there will not still be problems — if problems are going to occur, they usually present themselves within the first 90 days of operation.

It is important to tie the start of the warranty period to final cutover, *not* final acceptance.

STEP 4 SUPPORT AND MAINTENANCE

Goal: *To ensure the accepted system stays at optimal operational level during its life.*

Timing: *10-15 years, depending on the system life*

In This Step: *Establish maintenance procedures;*
Establish support procedures; and
Establish backup procedures.

Key Stakeholders: *CIO/CTO, IT Support Staff (Vendor and Agency), Maintenance Staff (Vendor and Agency), and End Users*

Key Deliverables: *Maintenance Plan, Support Plan, and Continuity of Operations Plan (COOP)*

Consider: *Public safety systems are designed to minimize the potential for outages. No matter how hard we try, however, systems still experience failure. What do you do when there is an outage? Having a COOP that can be put into play during an outage will help mitigate the impact to public safety. For more information visit the Federal Emergency Management Administration COOP Programs website at http://www.fema.gov/government/coop/index.shtm.*

1. SYSTEM SUPPORT

How does it work? The system has been installed and all the users trained, but there is still a period of time when the users must become acclimated to the new/upgraded system. Have a program in place to assist the users when they need help – they will call.

1.1. SUPPORT VERSUS MAINTENANCE

System support is often confused with system maintenance. *Maintenance* is used to fix something that is broken or prevent something from failing, while *support* is what is given to help the system operate and function. When negotiating the system contract, make sure you understand all your system support options.

- **Vendor Support** – One option is to continue the vendor support – this comes with a recurring cost.
- **Third-Party Support** – Another option is third-party local service company support, which would require a separate contracted agreement.
- **Internal Support** – This option, which involves the use of in-house support personnel, provides the highest degree of control over support issues.

1.2. APPLICATION SUPPORT

Software-driven – Modern communications systems are highly oriented toward software-driven applications. The various feature sets are typically driven by some manner of computer application. Software applications may be directly sourced by the prime vendor or may be provided by a third-party vendor.

1.3. USER SUPPORT

What do you do at 3:00 am when one of your field officers has difficulty initiating a field gateway patch? Consider the following:

- Do you have staff operating 24/7 and on-call?
- Do you have vendor support available 24/7?
- Is there a help desk available?

2. SYSTEM MAINTENANCE

Does it still work? A system is only as good as the ability to keep it running. Maintaining a system can be difficult and costly, but public safety cannot afford to be without a sound maintenance plan.

2.1. WARRANTY VERSUS MAINTENANCE

A warranty designates a negotiated period during which the vendor is required to support the system — it is traditionally never done with in-house support staff. This initial maintenance should be the responsibility of the vendor under the negotiated warranty period. As a result, the initial support cost should be very minor.

2.2. HARDWARE MAINTENANCE

Physical equipment is subject to breakage due to normal use and, as such, should be covered under some form of a maintenance plan. Suggested maintenance models include:

- **Vendor Maintenance** – The vendor will maintain the system in its entirety, and this becomes a recurring cost, including parts and labor.
- **Third-Party Maintenance –** A third-party local service company will maintain the system in its entirety, and this becomes a recurring cost — parts may or may not be included.

- **Internal Support** – The in-house maintenance personnel maintain the system, and the personnel cost becomes a recurring expense. Vendor support becomes time and material.

In all cases you should maintain required replacement/spare parts, which should be stocked locally to assure quick restoration following an outage.

2.3. SOFTWARE MAINTENANCE

Software-driven equipment is subject to periodic upgrades and should be covered under a maintenance agreement. These agreements can include two elements:

- **Periodic Maintenance Upgrades** – Address system issues.
- **Periodic Version Upgrades** – Address features and functionality.

Maintaining the software upgrades for communications systems will be part of a long-term life cycle program. Include it in your ongoing system plan.

2.4. PHYSICAL INFRASTRUCTURE MAINTENANCE

Develop a routine inspection program that reviews maintenance and security for all physical communications components, including shelters, buildings, towers, and the backup power system.

3. SYSTEM OPERATING PROCEDURES

What is the best way to use it? The system is installed and users are trained, but there are procedures that must be followed to ensure the best operational state. Users must understand the difference between knowing system capabilities and applying system capabilities correctly.

3.1. OPERATIONAL STANDARDS

Efficient mission operations are dependent upon establishing, maintaining, and enforcing proper system use and procedures. Operational protocols and procedures are an essential component of end user training. System operational protocols are an essential component of an agency. Standard Operating Procedures are essential documents that govern all areas of an agency's mission and should be maintained, reviewed, and revised on a regular basis.

- **Normal Operations** – This mode is often referred to as day-to-day operations and requires a simple and effective set of procedures that can be easily supported in the field.

- **Backup Operations** – This mode occurs as the result of a component or system failure. System operating procedures should be established to support backup operations and tie back to the COOP.

- **Emergency Operations** – There may be several cases that require reversion to emergency operating procedures. These include declared (and instant) operational emergencies such as natural or manmade disasters.

- **Regional Operations** – The system may be a single, multi-jurisdictional system covering an extended area of operation or a separate, connected part of an extended network of systems operated by other agencies. Regional operations may also include shared access to adjoining systems. Depending on the type of interactive system(s), the impact may be technical, operational, or both.

STEP 5 REFRESHMENT

Goal: *To ensure the system continues to support the user's needs over the system's useful life.*

Timing: *10-15 years, depending on the system life*

In This Step: *System Assessment; and Technology/System Refreshment*

Key Stakeholders: *Executive and Middle Management, IT Management and Staff, and End Users*

Key Deliverable: *Technology/System Refreshment Plan*

Consider: *Technology refreshment does not mean system replacement – if that is the case, you are circling back to Step 1. This step entails the necessary infusion of technology advancements due to external influences, such as a new standard or interoperability need.*

1. REVIEW

What can you do to make it better? The system as you planned it had to be installed and made operational even as newer and more advanced technology was released. This does not mean you missed out; however, it does require additional assessments and planning to ensure you infuse technology at the right time and without disruption.

1.1. SYSTEM ASSESSMENT

A full life cycle planning process includes continual reassessment of the system. This includes assessment of ongoing operational suitability, operational stability, and potential failure as well as an overall cost analysis, which takes into account capital expenditures, recurring costs, and maintenance costs. Pay special attention to all potential weaknesses, whether operational or

technical. Review the potential impacts of future demographic and operating environment shifts, such as including expansion of services and workforce, and areas of operation.

Periodic facilitated meetings of the various practitioners and stakeholders may provide focused insight to the state of the communications system and provide an opportunity for stakeholders to discuss changing needs and possible solutions.

1.2. TECHNICAL INNOVATION

Technical innovation provides opportunities previously unavailable. The rate of technical innovation is increasing at an exponential rate. While many new features are attractive, agencies must weigh any advanced features carefully. Identify the primary role of the communications system and how the inclusion of advanced features would impact that role. Be prepared to analyze the full cost/benefit of these features, noting that cost may not be in dollars but in secondary impact on personnel and basic operations. This includes assessment of ongoing operational suitability, operational stability, and potential failure as well as an overall cost analysis, which takes into account capital expenditures, recurring costs, and maintenance costs.

1.3. STANDARDS

Adherence to, and the understanding of, the various technical standards provides protection from isolation and obsolescence. Additionally, standards are the basis for successful interoperability. Project 25 (P25) is the commonly accepted standard for public safety communications systems (more information about P25 can be found at the Project 25 Technology Interest Group website at http://www.project25.org/). Remember: While technology is not the sole component of interoperability, it is a major facilitator of interoperability, and standards help make it work.

Standards are there for a reason, and it is important to know of their existence, understand their benefits, and ensure that they are considered as part of the life cycle of public safety systems. The more we adhere to standards, the closer we are to achieving seamless interoperability.

1.4. SYSTEM VERSION MANAGEMENT

Computer-controlled radio systems rely on very sophisticated computer systems and networks. Like all other aspects of conventional computer systems, many of the features, enhancements, and newer developments are reliant on periodic upgrades of the operating systems. Version upgrades are often sequential and require the installation of all intermediary version upgrades; thus, it is imperative that the upgrades be installed in a timely manner to avoid extensive costs and potential downtimes.

1.5.NATIONAL, STATE, AND REGIONAL INTEROPERABILITY INITIATIVES

Interoperability has evolved over the years and is now becoming more of a necessity than just a consideration. As systems are being considered, it is important to have awareness of what interoperability efforts are under way or being considered that may impact system design or advancements. More regional initiatives are taking shape, and many states have advanced interoperability by developing statewide radio systems, as well as gateway approaches that link regional and local systems via the "systems of systems" approach. There are also many interoperability programs that provide assistance and insight from a national perspective.

- **OEC** – OEC is working to improve interoperability and operability nationwide and has a wealth of programs available to Federal, state, local, and tribal agencies. Programs range from the Interoperable Communications Technical Assistance Program to the Border Interoperability Demonstration Projects. Website: http://www.dhs.gov/xabout/structure/gc_1189774174005.shtm

- **NECP** – NECP is the Nation's first strategic plan to improve emergency response communications, and [it] complements overarching homeland security and emergency communications legislation, strategies and initiatives.
  Website: http://www.dhs.gov/files/publications/gc_1217521334397.shtm

- **SAFECOM** – This is a communications program managed under DHS and is supported by OEC and the Office for Interoperability and Compatibility.
  Website: http://www.safecomprogram.gov

2. ADOPTION OF ADVANCING TECHNOLOGY

How do we get the new stuff? Public safety personnel must be mindful of the environment in which we operate and consider that, for all intents and purposes, we are not usually the first to adopt new technology. The risk of jumping in too soon is significant. Driving innovation is fine, but make sure you clearly understand the potential impacts before you make the leap.

2.1. EARLY ADOPTION

Consider a technology maturity model, as shown in Figure 8, and determine where the technology you are considering falls on the curve. Public safety mission-critical systems have very stringent system survivability requirements that make early technology adoption difficult — tried and tested is a more reliable model. However, there are certainly new technologies for which public safety entities can and should be the innovators, and they should consider adopting these technologies to improve response and recovery without impacting the mission-critical nature of the system.

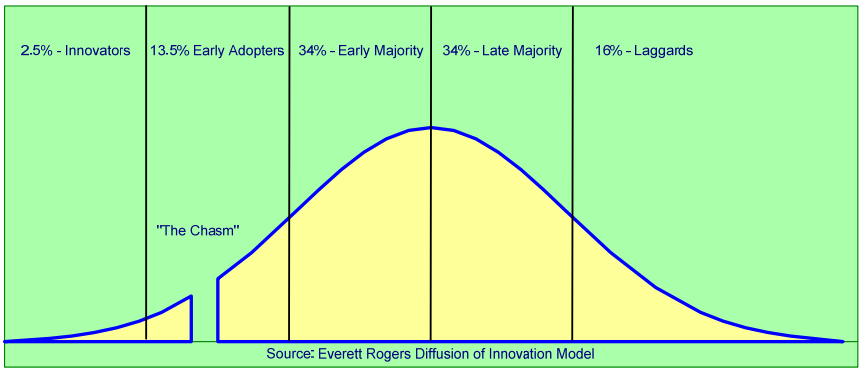


Figure 8 – Technology Adoption Model[3]

2.2. TECHNOLOGY MATURITY

Technology Planning – Look toward technologies that advertise a forward migration strategy with minimal stranded system exposure. As part of your ongoing life cycle planning and review, include a review of the state of the technology in use and emerging technologies.

[3] Rogers, Everett M. *Diffusion of Innovations*. Glencoe: Free Press, 1962.

STEP 6 DISPOSITION

Goal: *To ensure the old system components are disposed of without adverse impact to the operations of the new/upgraded system.*

Timing: *90 days after the cutover to the new/upgraded system*

In This Step: *System Asset Disposal*

Key Stakeholders: *Middle Management, Project Management, Lead Agency, and Finance Staff*

Key Deliverables: *Disposal Plan and Capital Asset Depreciation Form*

Consider: *Disposal does not always mean to throw away. Other agencies within your jurisdiction or in other areas may have a need for used equipment. Consider Government surplus websites that offer to host the sale of your used equipment.*

1. DISPOSITION PLAN

It was good while it lasted, but now how do we get rid of it? Disposal is the least considered step in life cycle management and can present some very good opportunities; however, it can also create some problems if not done carefully. Take some time to weigh the options for disposal and ensure that there will be minimal impact to the operations of your new/upgraded system.

1.1. REUSE

Review those components that have extended life value and could be reused in a new communications system. Be careful that reuse does not interject a potential, and avoidable, "Achilles heel" into an otherwise new system. Address system failure points as part of your risk management.

1.2. REPURPOSE

Careful consideration needs to be given to repurposing old equipment. Consider turning over incumbent systems to other departments or service units that would otherwise not qualify for operating on the new system but still could benefit from any residual life of the old system. However, be careful not to do more harm to interoperability than intended — older radios and radio systems may not be able to communicate on the newer system. If this is a consideration, be sure to account for solutions that will allow the old radio systems to interoperate with the new system.

1.3. SPACE AVAILABILITY

Space consideration will include the physical capacity of equipment shelters and antenna loading on towers, as well as power capacity and heating and cooling. Installations may be subject to tight quarters during the initial migration. Superfluous equipment should be removed and systems cleaned up accordingly within the timeframe of your transition plan.

During the cutover and migration phase of system implementation, you will need additional space to house infrastructure equipment for the old and new systems. Another factor is the additional cost of maintaining both systems.

Include in your migration planning a review of the operation and decommissioning of the infrastructure equipment. If you are considering keeping some or all of your old system, be sure to address space issues before and after transitioning to the new system.

1.4. DEPRECIATION

Include in your process an analysis of the remaining life of the incumbent system. Even in public sectors, it is good business practice to manage property by expectant life versus financial value. All agencies have to answer to an accounting entity, and it will make your job much easier if you have addressed the usable life of the equipment in light of any pre-existing amortization schedule. If the old system or equipment was classified as capital, be sure to document the disposition of the assets so that it can be fully depreciated.

1.5. SURPLUS PROPERTY

Before conveying surplus equipment to local agencies, closely scrutinize the impact. Will the equipment truly meet the needs of the recipient agency? Will use of the equipment be consistent with agency and regional emergency communications plans and goals and meet interoperability requirements? Or will the equipment potentially isolate receiving agencies? Request assurances that the equipment will be used as intended and put into active service. Be realistic with the receiving agencies on the expected service life of the equipment and its suitability for the intended service.

Adopting excess equipment from larger agencies has long been a popular tactic among smaller agencies/departments, particularly the volunteer fire, EMS, and search and rescue communities. This is a good method of stretching tight budget dollars. Trade-in value for new system procurement has rarely been of any real advantage to vendors and is thus of minimal financial impact to donor agencies.

FINAL THOUGHTS

A public safety system is one of the more complicated mission-critical systems deployed in the Nation, and, as such, the life cycle management of these systems is no small task. It can often take three years just to go from **STEP 1 – PLANNING** to the completion of **STEP 3 – IMPLEMENTATION**. If you take into consideration the useful life of the system (an additional 10 years or more), it is a very large investment in time, not to mention money. Yet although the commitment is significant, the benefits far outweigh the costs, because the systems are crucial in ensuring that public safety personnel can communicate effectively during any emergency, thereby helping speed response and reduce loss of life and property.