Emergency Communications System Lifecycle Planning Guide

Publication: July 2025
Cybersecurity and Infrastructure Security Agency

Table of Contents

Introduction *1*

Continued Need for LMR and Communications Funding 3

Emergency Communications System Lifecycle Phases *4*

Phase 1: Pre-Planning | 6 - 12 Months 4
Recommendations 4
Key Considerations 7

Phase 2: Project Planning | 6 - 18 Months 8
Recommendations 9
Key Considerations 11

Phase 3: Request for Proposals and Aquisition | 6 - 12 Months 12
Recommendations 12
Key Considerations 14

Phase 4: Implementation | 18 - 24 Months ..... Error! Bookmark not defined.
Recommendations 16
Key Considerations 19

Phase 5: Support, Maintenance, and Sustainment | Year 1 – Year 25 21
Recommendations 22
Key Considerations 29

Phase 6: End-of-Lifecycle Assessment and Replacement | Year 7 – Year 25 30
Recommendations 30
Key Considerations 33

Phase 7: Disposition | 90 Days After Cut-Over or Transition 33
Recommendations 34
Key Considerations 35

Conclusion *36*

About SAFECOM/NCSWIC *36*

Appendix: Definitions *37*

Introduction

The Cybersecurity and Infrastructure Security Agency (CISA) 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. In support of its mission, CISA collaborates with SAFECOM and the National Council of Statewide Interoperability Coordinators (NCSWIC) to ensure public safety stakeholders drive content in guidance documents intended for the entire public safety community. This collaboration resulted in this *Emergency Communications System Lifecycle Planning Guide* (referred to hereafter as the *Lifecycle Guide*), which defines system lifecycle phases (**Figure 1**), goals and products, stakeholder involvement, roles and responsibilities, and items for consideration in each phase. The *Lifecycle Guide* provides recommendations for agencies interested in building, maintaining, and operating an emergency communications system through decommission and replacement.[1]

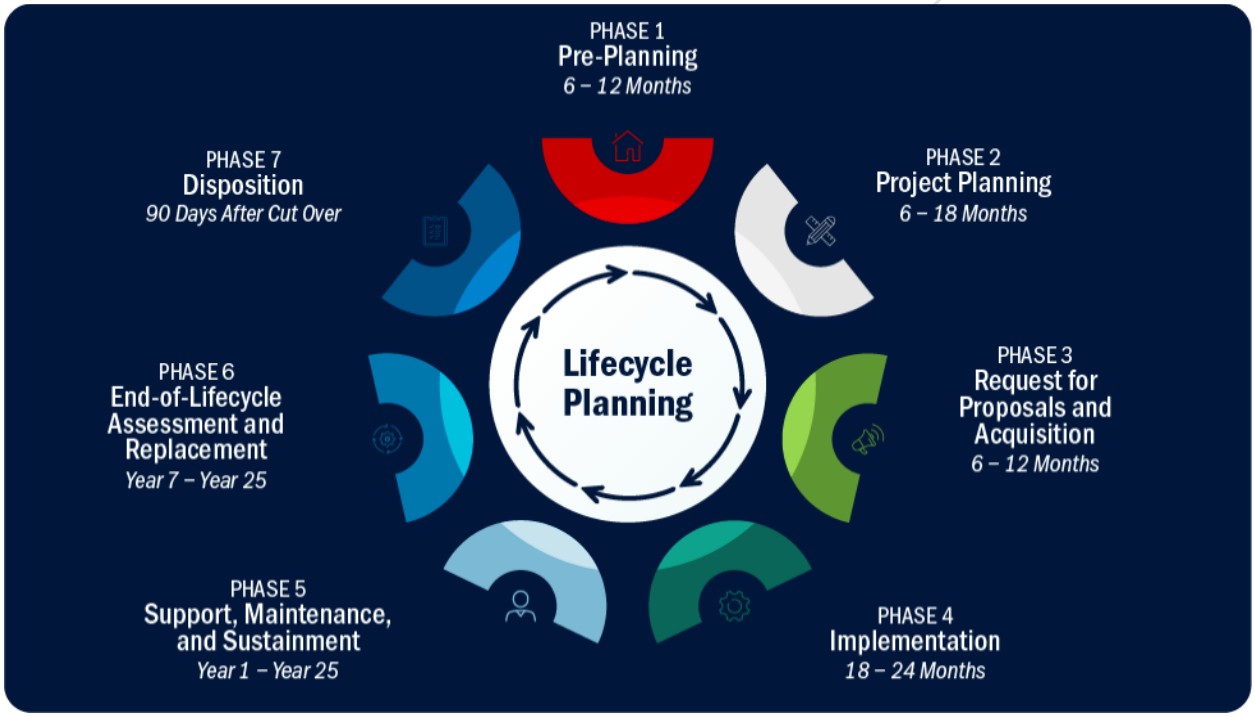


Figure 1: System Lifecycle Planning Model

Each phase of the system lifecycle planning model—Pre-Planning; Project Planning; Request for Proposals and Acquisition; Implementation; Support, Maintenance, and Sustainment; End-of-Lifecycle Assessment and Replacement; and Disposition—includes best practices, considerations, and recommended checklists to assist public safety agencies embarking on system lifecycle planning. Specifically, the checklists are designed to be torn-out, referenced, and used by project management teams throughout the system lifecycle. **Table 1** summarizes the system lifecycle planning model phases and high-level recommendations contained in this document.

[1] The system lifecycle planning model is based on a Technology Lifecycle Management (TLM) model. This document takes into consideration existing relevant emergency communications lifecycle planning documents, as well as industry best practices for lifecycle planning methodologies such as Closed Loop Lifecycle Planning, System Development Lifecycle, and TLM.

Table 1: System Lifecycle Planning Model and Recommendations Summary

Planning Model	Recommendations
Phase 1: Pre-Planning **Timing:** 6-12 months **Goals:** Inform and secure the decision to replace, upgrade, maintain, dispose of, and/or acquire a new system	• Establish the core planning team • Research and develop system and funding options • Decide on the optimal and alternative solutions with funding options • Plan for frequency needs and channel programming • Develop a business case, presentation materials, and strategic plan • Identify a legislative- or executive-level project champion • Present to decision-makers and secure funding to support the initial build-out and sustain the system throughout the entire lifecycle
Phase 2: Project Planning **Timing:** 6-18 months **Goals:** Formalize the project team; identify operational and technical requirements for system replacement and upgrade; and develop the project plan	• Consider how long the planning process can take and communicate expected timeframes to elected officials • Collect user needs and requirements and incorporate into project plans • Engage with communications leaders early for guidance and support (e.g., Statewide Interoperability Coordinators [SWIC], Statewide Interoperability Governing Bodies [SIGB] if required) • Identify strong Project Sponsors (e.g., state or local elected officials) • Begin planning the Request for Proposals (RFP)
Phase 3: RFP and Acquisition **Timing:** 6-12 months **Goals:** Select the appropriate procurement vehicle and procure systems and components	• Develop a written action plan • Form the RFP team • Develop the Statement of Work (SOW) • Include specifications or requirements in the RFP • Establish written evaluation criteria well before the award • Conduct a formal objective review process and document results
Phase 4: Implementation **Timing:** 18-24 months **Goals:** Develop an implementation plan; install new systems; test; train users; and transition from legacy to new	• Develop the implementation plan • Understand and document testing procedures (e.g., factory testing, staging, site installation and testing, coverage verification, testing and acceptance, cut-over, final acceptance) • Update operational procedures and train users • Promote new communications capabilities and benefits to the community
Phase 5: Support, Maintenance, and Sustainment **Timing:** Year(s) 1-25* **Goals:** Inventory and maintain equipment; manage budget; and assess and communicate needs	• Maintain an accurate inventory of equipment (e.g., scope, database tool, inventory team, processes to compile and secure data) • Determine and execute an ongoing maintenance and operations model • Manage the budget when the project is conceived, directly before it is funded, and after delivery • Share communications needs with decision-makers early and continually

Planning Model	Recommendations
Phase 6: End-of-Lifecycle **Timing:** Years 7-25* **Goals:** Determine when to replace systems or components with solutions to best fit operational and technical needs	• Conduct ongoing assessments of current system (e.g., implement a balanced scorecard) to plan for technology maturity • Refresh or upgrade systems, as needed, to extend the life of the system • Determine potential replacement solutions, with consideration to support national, state, and regional interoperability initiatives; consider early adoption of new technologies; and adhere to widely used technical standards
Phase 7: Disposition **Timing:** 90 days after cut-over or transition **Goals:** Determine options and dispose of legacy systems or components	• Develop the disposition plan • Determine options (e.g., reuse or repurpose old components, consider space availability, convey surplus equipment to partner agencies) in consideration of legal or policy limitations, and business requirements • Brief leaders on disposition plans • Identify lessons learned following disposition

*Timelines provided are estimates and may differ depending on individual jurisdictions and implemented technologies.

Public safety agencies are experiencing an increase in data shared across jurisdictions, disciplines, and agencies at various levels of government. This creates the need and opportunity for public safety agencies to increasingly coordinate with other agencies. Many agencies are already working together to incorporate advanced technologies to support regional systems and to develop formal governance structures, joint processes, and procedures to improve emergency communications and response.[2] This increased level of coordination and complexity affects system lifecycle planning, especially as agencies prepare to integrate systems and share infrastructure, equipment, and costs.

CONTINUED NEED FOR LMR AND COMMUNICATIONS FUNDING

Emergency communications technologies continue to evolve at a rapid rate, further complicating lifecycle planning and decisions regarding system upgrades and replacements. Public safety agencies operate, deploy, or contract services for communications including land mobile radio (LMR), public safety broadband and internet protocol (IP)-based technologies such as FirstNet[3] and other broadband service providers, satellite, information technology (IT) networks, alerts, warnings, and notifications, and many more systems that enable personnel to access, transmit, and share important data. While public safety agencies are excited to adopt advanced technologies and improve data capabilities, they must balance the costs for mission critical capabilities.

As a result, many agencies have prioritized maintaining LMR systems and other emergency communications capabilities gained in recent years as they gradually adopt and deploy IP-based technologies and services for data access and transmission.[4] This convergence of technologies presents new challenges for public safety agencies responsible for maintaining and financing these systems.

[2] For governance best practices, see the CISA *Governance Guide for State, Local, Tribal, and Territorial Officials*.
[3] For more FirstNet information, see the First Responder Network Authority website at: firstnet.gov.
[4] See the CISA *Public Safety Communications Evolution* brochure at: cisa.gov/resources-tools/resources/lmr-and-broadband-evolution.

The environment is extremely complex, and technology is evolving quickly, making it difficult for public safety agencies to assess technological and financial options for communications systems. Decision makers are also struggling to understand new technologies' features and limitations as well as their funding implications. To address these challenges, CISA, SAFECOM, and NCSWIC developed a trio of documents on LMR technologies to inform decision makers and identified options for funding public safety communications systems.[5] These documents emphasize the need to sustain LMR systems and clarify funding requirements for ongoing maintenance, operations, and upgrades—not simply initial capital costs.

To further assist public safety stakeholders, CISA, SAFECOM, and NCSWIC collected examples of funding approaches and compiled the *Funding Mechanisms Guide for Public Safety Communications Systems*. It provides an overview of several methods of funding (e.g., bonds, taxes, grants) and examples of how these methods were used in state and local systems. These funds can be used for planning, capital costs, ongoing costs, refreshments, upgrades, and replacements. The funding mechanisms guide also provides examples of cost-saving methods, including innovative financing programs and information on shared systems.

Emergency Communications System Lifecycle Phases

PHASE 1: PRE-PLANNING | 6 - 12 MONTHS

As the first step in the *Lifecycle Guide,* the goal of the Pre-Planning phase is to inform and secure the decision and funding needed to replace, upgrade, maintain, dispose of, or acquire a communications system. A key take-away in this phase is to identify funding options not just for the initial capital investment, but for the entire system lifecycle (e.g., acquisition, maintenance, and upgrades), and to secure funding commitments before proceeding to the Project Planning phase.

Recommendations

The following recommendations are provided to assist public safety agencies embarking on communications system planning:

Establish a core planning team. The core planning team may be comprised of the SWIC; agency officials; technical staff; affected users; and procurement, financial, and legal staff. The core planning team should include representatives of agencies affected by the project who have full authorization to participate on behalf of the agencies they represent. The team should consist of a combination of key personnel from the technical and operational areas and include (i) Executive or Steering Committee; (ii) User Committee; (iii) Technical Committee; and (iv) Ad Hoc Working Groups. **Identify the problem, needs, and requirements.** Project planners should investigate the current system faults, user needs, and project requirements, such as:

- Diminishing performance of current systems or equipment
- End-of-lifecycle or lack of availability of replacement equipment

[5] SAFECOM/NCSWIC documents, including the *Funding and Sustaining LMR: Materials for Decision-Makers* and the *Funding Mechanisms Guide for Public Safety Communications Systems,* are available at: cisa.gov/safecom/funding.

- Staffing for implementation and sustainment
- Whether maintenance costs outweigh replacement costs
- Lack of coverage or capacity for critical users
- Need to close gaps in capabilities or improve capabilities
- Desire to add new users
- Cost-efficiencies that could be achieved by the proposal
- Expertise needed for the project

Research system options. Project planners may choose to develop and release a Request for Information (RFI). An RFI is a formal, non-binding request for information about current technologies and services offered by vendors based on functional requirements and user, business, and system needs and requirements set by the entity. RFIs help agencies gain a better understanding of solutions, services, and options to determine the appropriate procurement method and draft associated solicitation documents.

Research funding options. Project planners should review the *Funding Mechanisms for Public Safety Communications Systems*, which provides examples of funding methods to support planning, capital, replacement, and ongoing costs for public safety systems. The document also provides examples of states and localities that utilize various funding methods to pay for system upgrades, replacements, and ongoing costs.

Determine an approach. Project planners should evaluate both technical system and funding options and decide on a limited set of approaches (1–3) to present to decision-makers. The team must fully understand options, including strengths and weaknesses, and clearly convey information. Experienced officials caution that planners frequently approach decision-makers too early in the process, before the team has assessed user requirements and understands all options. Best practices for evaluating approaches include:

- Research and record options in writing before approaching decision-makers
- Weigh strengths and weaknesses of system options and feasibility of funding
- Develop consensus on an optimal approach and "next best" approaches
- Create a one-page fact sheet on basic requirements, recommended approach, and summary of alternative approaches; reference the *System Lifecycle Planning Tool*

Plan for frequency needs and channel programming. To use communications systems effectively, responders must have access to channels used for all types of events, including multi-disciplinary and multi-jurisdictional response. Planning radio channel usage and programming interoperability channels into equipment in advance of an emergency or planned event enhances preparedness. If communities plan their communications systems and operations to meet only their perceived immediate needs, they will be less able to give or receive assistance. Interoperability in the form of mutual aid to adjacent jurisdictions, other disciplines, or assistance to distant areas suffering a major disaster requires advanced planning, including interoperable communications pre-programming.

CISA published the *Programming Guide and Template for Interoperability Channels* to assist technicians to program radios. The template is consistent with the Federal Communications Commission and the National Telecommunications and Information Administration rules and

regulations, and the National Public Safety Telecommunications Council's standard channel nomenclature.

Create a business case, talking points, and marketing materials. Before discussing with decision-makers, project planners should develop a business case outlining why the system should be funded. A successful business case must demonstrate the value of the interoperability effort, provide a clear picture of the future of interoperability in the community, and speak to the interests and concerns of community leaders. CISA published guidance to help stakeholders develop effective business plans for interoperability projects in the *Interoperability Business Case: An Introduction to Ongoing Local Funding*. This guidance helps emergency response officials develop a compelling business case by presenting steps and considerations to follow and to tap into local funding sources.

In addition to creating a strong business case for funding purposes, project planners and the core planning team should develop simple talking points on the business case to present to decision-makers and funders. Developing talking points helps ensure the whole team is involved in creating a business case, and the message regarding needs and options is comprehensible and consistent. Lastly, project planners should develop concise marketing materials to inform decision-makers, funders, and their staff. Materials left with decision-makers or funders should be concise, so decision makers can easily understand the problem and recommend solutions as well as consider alternatives.

Identify executive-level project champions. Once project materials are created, project planners should identify one or more "champions" to review presentation materials, provide professional input on messaging and approach, help usher the project through executive and legislative processes, and manage roadblocks. Experienced officials report how champions have helped the core planning team:

- Incorporate useful advice into the project and presentation materials
- Connect to state and local experts (e.g., technical, procurement)
- Coordinate with other initiatives and partners who could support the project
- Gain access to leaders and elected officials
- Learn about state and local funding processes

Present proposal to decision-makers. After consultation with the team and project champion(s), project planners should begin to communicate, through formal and informal means, the proposal with decision-makers to obtain necessary approvals and funding. With the help of the project champion(s), planners should gain access to key officials, navigate the local decision-making process, and build support for the proposal.

Key Considerations

Timing for the Pre-Planning phase can vary greatly depending on the status and coordination history of emergency communications leaders and governing bodies across the whole community. Ideally, agencies should begin pre-planning activities several months to a year *before* funding is needed. Project planners should consider the following when developing project plans and securing funding:

Proposals cannot be funded immediately. Experienced officials report securing funding for a communications project often takes a year or more. This is due to the ongoing nature of state and local budget processes, which are often finalized long before an annual budget is passed. Agencies seeking funding need to understand the relevant funding cycle and determine (with state and local leaders, or their champion) the optimal timeframe for submitting a funding request, and when funding will be allocated (if approved). Many factors drive the amount, availability, and access to funding, including:

- Federal budget cycle and grant deadlines
- State/local budget cycles and timelines for submitting project proposals or budget requests
- Mandated programs or pre-determined priorities (funding already allocated to other projects)

Strategic plans provide context for decision-makers. A strategic plan should establish a single, overarching goal for improving public safety communications. The plan should then divide a large communications initiative into several smaller projects that could be funded and implemented in phases over time. This allows decision-makers to understand how each smaller project is an integral part of a larger plan. Experienced officials recommend dividing projects into phases to help an agency effectively manage the project – both technically and financially.

Communications projects compete for funding. State leaders are aware of the importance of emergency communications for public safety; however, they are charged with creating a budget addressing a variety of state and local needs beyond emergency communications. Project planners must be fully prepared to provide decision-makers with a written proposal, including benefits to the community, and promote confidence in the project and the core planning team.

Agencies must proactively assess and present requirements before a system fails. Project planners should continually assess needs and end-of-lifecycle indicators (e.g., lack of available replacement parts, end of production on equipment, cost of maintenance outweighing replacement costs) to anticipate system requirements. Experienced officials recommend maintaining relationships with vendors to forecast lifecycle needs and stay informed about equipment availability and issues affecting system upgrades. Project planners should update state and local governing bodies (e.g., Statewide Interoperability Governing Body [SIGB] or State Interoperability Executive Committee [SIEC]) if required and communications leaders (e.g., SWIC, State Administrative Agency [SAA]) on the status of systems and proposed projects. These governing bodies and leaders are the first step to coordinating proposals and ensuring alignment with the area's strategic plans (e.g., Statewide Communication Interoperability Plan [SCIP], broadband deployment plans).

Checklist: Pre-Planning Phase	
☐	**Establish the core planning team,**[6] with the right mix of experts (e.g., technical, financial, legal, procurement, users) to define needs and basic requirements, research and develop system and funding options, and determine optimal approaches
☐	**Identify the problem, needs, and requirements**, such as diminishing performance of current systems; lack of availability of replacement equipment; cost of maintenance outweighs replacement; lack of coverage or capacity for critical users; need to improve capabilities; desire to add new users; and potential cost-efficiencies that could be achieved
☐	**Research system and funding options** – Develop and release a Request for Information (RFI) to solicit input on system capabilities – Reference the *Funding Mechanisms Guide for Public Safety Communications Systems* to understand methods for capital and ongoing costs; develop funding options for entire system lifecycle; and seek cost-saving methods (e.g., asset sharing)
☐	**Determine an approach** – Research and record options in writing before approaching decision-makers – Weigh strengths and weaknesses of system options and feasibility of funding – Develop consensus on an optimal approach and "next best" approaches – Create a one-page fact sheet on basic requirements, recommended approach, and summary of alternative approaches; Reference the *System Lifecycle Planning Tool*
☐	**Plan for frequency needs and channel programming** to include various interoperability channels. Reference the *Programming Guide and Template for Interoperability Channels*
☐	**Create a business case, talking points, and marketing materials** to outline the proposal and ensure consistency and clarity in messaging. Reference the *Interoperability Business Case: An Introduction to Ongoing Local Funding*
☐	**Identify executive-level project champions**, and seek review and input on technical approach, funding options, and presentation materials
☐	**Present proposal to state or local decision-makers**, after consultation with the project champion(s)
☐	**Secure funding to support the initial investment and sustain the system** throughout the entire lifecycle

PHASE 2: PROJECT PLANNING | 6 - 18 MONTHS

[6] Pre-planning is usually conducted by existing staff or consultants. While consultants can assist in the process and can provide subject matter expertise (e.g., financial, legal), it is essential for the agency to be involved in the pre-planning process to define requirements, set project goals, and make major decisions. By participating in this process, project planners will be able to describe and defend decisions to decision-makers.

PHASE 2
Project Planning | *6 – 18 Months*

The *Lifecycle Guide* emphasizes system planning that occurs after a strategic decision has been made to replace, upgrade, maintain, dispose of, or acquire a system. Once the strategic decisions have been made, and the Pre-Planning phase is complete, then Project Planning can begin. The goals of the Project Planning phase are to (i) formalize the project management team; (ii) identify and approve the operational and technical requirements for system replacement or upgrade; and (iii) develop the project plan to include key elements such as the purpose, objectives, timeline, and budget.

Recommendations

The following recommendations should be considered during the Project Planning phase:

Document user needs and requirements. The core planning team should engage with a wide array of system users from all agencies impacted by system replacement or updates to understand communication users' needs and requirements. By engaging with users early in the planning process, the team will be better able to define gaps and needs and shape the process to meet user needs.

Engage with communications leaders for guidance and support. Project planners should engage with statewide governing bodies and communications leaders, such as the SWIC, if not already part of the core planning team. The SWIC can ensure the project supports statewide plans and initiatives, help the team connect with state, regional, and local agencies with similar projects underway, and foster asset-sharing, joint procurement, and partnerships with other agencies and jurisdictions. By working with statewide governing bodies and SWICs, the team can strengthen proposals and increase their chances of securing support and funding.

Identify strong project sponsors. The *Lifecycle Guide* identifies the need for a project sponsor who can help the core planning team secure support and additional funding for the project from senior-level state leaders (e.g., Governor), and state and local elected officials. Often, project management teams recruit state or local elected officials to serve as project sponsors because they have: (i) a commitment to improving community services; (ii) working relationship with senior-level executives; (iii) strong communication skills; and (iv) the ability to secure additional funding, as needed. Project sponsors should bring:

- Some subject matter expertise relevant to the project and passion for the cause
- Access to senior-level executives and subject matter experts (e.g., financial, legal, technical)
- Strong communication skills
- Experience developing funding and financing proposals
- Awareness of surrounding systems to help inform potential opportunities for partnerships, asset-sharing, and resource sharing
- Experience managing projects and identifying and mitigating risks

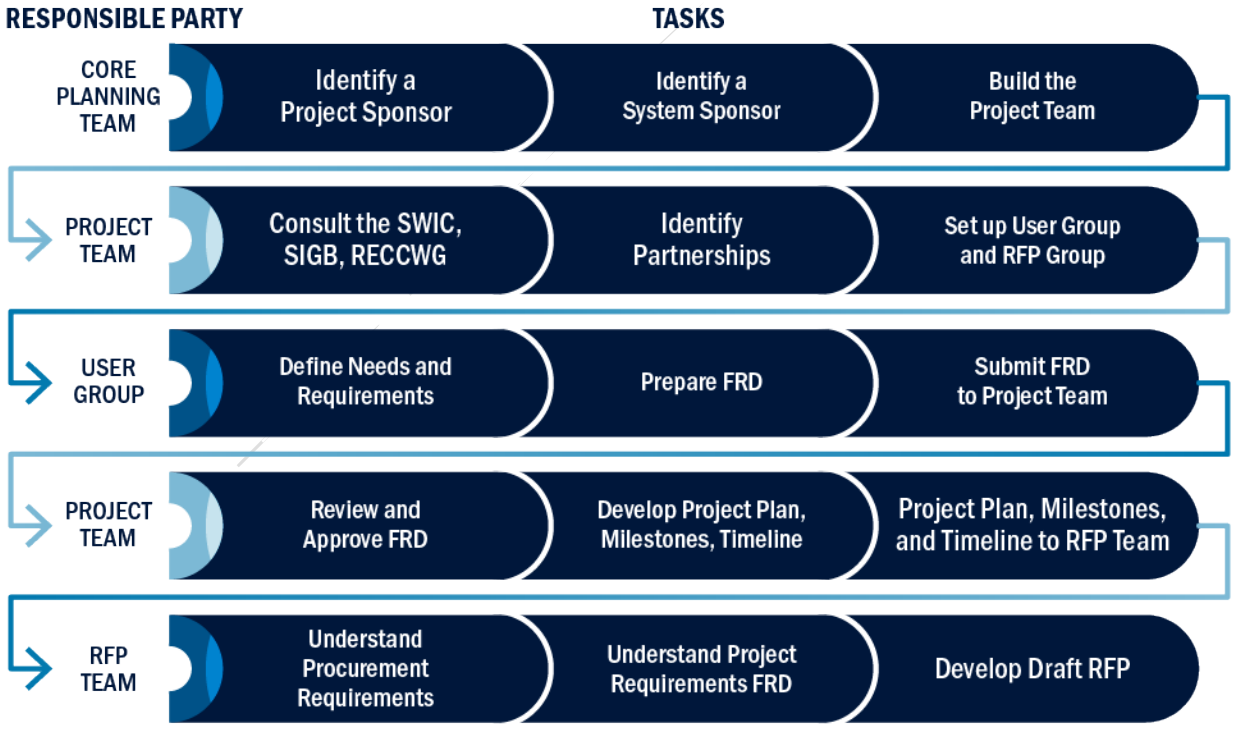
The core planning team should complete initial planning (see Pre-Planning phase) and scoping of the project before identifying and engaging with a project sponsor. This allows the team to develop its own thoughts on an approach (e.g., upgrade, replacement, or refreshment), select the best and alternate options, and identify funding sources for the selected approach. With a unified front, the

team can effectively present its proposal and written materials to the project sponsor(s) and solicit his or her feedback and support.

Once the project has support, the core planning team can proceed with the formal Project Planning phase activities, including (i) building a project management team; (ii) developing a project plan; (iii) defining functional and technical requirements; and (iv) documenting the requirements in a Functional Requirements Document (FRD).

Begin planning the Request for Proposals (RFP). Experienced officials recommend forming an RFP team during early planning, comprised of a variety of experts (e.g., legal, financial, procurement, grant, and communications technicians). See the RFP and Acquisition Phase for additional guidance on forming the RFP team. This RFP team should establish an action plan and preliminary timeline for developing the RFP and communicate that timeline to the core planning and project management teams.

Before drafting the RFP, the team should consult state and local procurement offices, as well as past RFPs, to understand the state or local RFP process, procurement requirements, confidentiality and non-disclosure requirements, and the typical process and timeline for RFP approval. Additionally, the RFP team should become familiar with the project – the general approach, funding options, services and products needed, specific technical and operational requirements in the FRD, foreseeable risks, and any necessary sequence of events. Lastly, the RFP team should reference the formal project plan (once complete) to set preliminary milestones and dates in a draft RFP. See **Figure 2** for recommended Project Planning Phase activities leading to RFP development.



p

Figure 2: Project Planning Phase Process and Responsibilities

Key Considerations

Experienced officials have noted that project planning can take from 6 to 18 months[7] to plan all aspects of the project, educate decision-makers, and secure a commitment of funding if not already accomplished during the Pre-Planning Phase. Due to the length of this phase, project planners should be funded separately, and not as part of a grant providing funding for the communications system, if applicable. Grants have a set period of performance, and if planning activities are delayed, then agencies may not be able to complete system acquisition and are at-risk of losing grant funding. Agencies should conduct planning before requesting grant funding or apply for supplemental grants and acquisition funds near the end of the Project Planning phase. Agencies should also consider which tasks should be handled by internal experts and which may be contracted to expert third parties.

Checklist: Project Planning Phase	
☐	**Ensure appropriate time for project planning (typically 6-18 months)** – Review past projects to learn how long the Project Planning phase has taken for other projects in your agency, jurisdiction, and region – Build sufficient time for planning into project work plans (given the time it takes for environmental planning and historic preservation review, zoning review, state/local legislative reviews, optimal times to request funding) – Communicate the expected project timeline to elected officials, including the time needed to adequately plan the project
☐	**Document user needs and requirements** – Engage with system users early – Collect user needs and requirements – Determine how user needs may affect project timelines and system costs – Document user needs and requirements in project materials
☐	**Engage with communications leaders for guidance and support as necessary or required,** including – Statewide Interoperability Coordinator – Statewide Interoperability Governing Body or State Interoperability Executive Committee – Regional Emergency Communications Coordination Working Groups – Federal Communications Commission to coordinate spectrum/licensing issues – Elected officials
☐	**Identify strong project sponsors** after Pre-Planning Phase activities are complete, but before engaging in formal project planning (e.g., developing work plans, budgets) – Identify an executive-level leader who has knowledge of the state or local legislative process, procurement processes, and funding options – Share project materials with project sponsors – Gain feedback on products and messaging – Support the project sponsors in meetings with elected officials, decision-makers, and funders

[7] Experts report state and local legislative review and approval processes, as well as environmental and historical preservation review processes, can extend this timeframe.

Checklist: Project Planning Phase	
☐	**Begin planning the Request for Proposals** – Identify experts (e.g., legal, financial, procurement, grant, technical) for the RFP team – Examine past RFPs and approval processes – Reference the project plan for dates, milestones, and timelines to include in the draft RFP – Incorporate the planned RFP development and review timelines into the project plan – Communicate planned RFP timelines to the core planning and project management teams

PHASE 3: REQUEST FOR PROPOSALS AND AQUISITION | 6 - 12 MONTHS

The *Lifecycle Guide* provides guidance on RFP development and acquisition, which is the third phase of the system lifecycle planning model. This phase includes identifying specific costs associated with emergency communications projects (e.g., backhaul sites, subscriber units, consoles, peripheral equipment, system interfaces), as well as ongoing costs (e.g., software upgrades, hardware repair or replacement, leasing fees, warranties, programming costs, training, refreshment). The goals of the RFP and Acquisition phase are to select the appropriate procurement vehicle (e.g., Full and Open Competition, Sole Source), oversee an objective review process, and procure necessary systems and system components.

Recommendations

The following recommendations should be considered during the RFP and Acquisition phase:

Obtain full approval from appropriate officials and funders (if applicable) on the project before drafting the RFP. The overall strategy should be approved by elected officials ***before*** the RFP and Acquisition phase is started.[8] Initial RFP planning should begin early, with the formation of an RFP team to review past RFPs and approval processes, as well as the project plan, to determine development timelines.

Develop an action plan. Project planners should develop an action plan for developing their RFP. Developing an action plan will help the sponsoring agency think through the RFP process – who needs to be involved, how long it will take, what requirements should be included in the RFP, and what the key milestones are to indicate progress. As part of their action plan, planners should include time to:

- Form an RFP team
- Set expectations for confidentiality
- Understand procurement rules and timelines
- Develop a clear understanding of services and products needed
- Set milestones for the procurement schedule

[8] Some agencies report they have approached officials after the RFP is complete so they can provide more details for decision-makers; however, most public safety leaders advocated for full approval and buy-in before the RFP process begins to raise awareness of the project and to save time and money if the project is ultimately not supported.

Form the RFP team. If not already completed during the Project Planning phase, the core planning team should form an RFP team to manage the RFP process. The team should include:

- **Procurement Manager:** This person is assigned to manage the RFP process on behalf of the agency procuring the system or components, from leading the development of the RFP, through contract negotiation, award, and purchase.
- **Procurement Officer:** This is a person (or office) assigned to oversee adherence to the state's procurement code and provide oversight of the process, from issuance of the RFP through award and possible protest.
- **General Counsel:** Ensures legal sufficiency of any contract terms and conditions as part of the RFP, and in negotiating terms.
- **Program Manager:** The person from the sponsoring agency responsible and accountable for the services and products to be procured.
- **Subject Matter Experts:** People with expertise (e.g., financial analyst who can evaluate bids) to advise during the RFP process, from the evaluation, financial decisions, award, and possible protest.
- **Evaluation Committee:** This is a group of people from various backgrounds who will participate in the evaluation of RFP vendor responses. This can include the program manager, such as an agency head, technical staff, and the project manager. The committee could also include advisory staff supporting the evaluation process, such as a financial expert, a legal expert, and/or a procurement expert. While these experts would not be "voting members" of the committee, they could advise during evaluation.

By forming a diverse RFP team of experts, project planners will be able to: (i) manage the RFP process, (ii) ensure user needs and requirements are incorporated, (iii) comply with legal and procurement rules, and (iv) develop a strong RFP to yield the best possible procurement for the sponsoring agency.

Develop the Statement of Work (SOW). The SOW sets the tone for the project and expectations for the bidders, including the scope of work, objectives, deliverables, and timelines. The SOW should include clear and helpful information to support development of the RFP specifications and evaluation criteria to easily identify the differences between vendors. Additionally, the SOW should allow some vendor flexibility in the proposed solutions for the work, services, or products and ensure vendors meet the procuring agency's minimum requirements.

BEST PRACTICE
Identify all requirements to ensure essential procurement needs are met.

Include specifications or requirements in the RFP. It is essential the people selected for the RFP team have sufficient knowledge, expertise, and experience writing RFPs. When developing an RFP, the language should be clear and concise. The RFP team should:

- Review and compare user requirements (collected in Pre-Planning and Project Planning phases) in the SOW with the terms and conditions included in the RFP to ensure they are consistent.
- Build the list of functional requirements to support the solicitation.

- Use generic or nonproprietary language, when appropriate. This reduces the risk of a potential protest where it may be perceived the RFP is leaning toward a particular company or product.
- Be careful with the words “shall” and “should.” The word “shall” is a binding term on the Contractor. The word “should” mean something is recommended but not mandatory.
- Include definitions for any acronyms or technical and special terms used in the RFP.
- Avoid unclear or vague language by using simple language to minimize confusion.

Vendors must clearly understand specifications or requirements in the RFP so they can respond with appropriate proposals. In addition, responses will be more targeted to the agency’s needs, more easily compared during evaluation, and evaluation will be more objective. When developing specifications for vendors, the RFP team should:

- Identify minimum requirements for vendors (i.e., the must-haves)
- Ensure non-price requirements are at no added cost
- Include technical standards to ensure interoperability is established/maintained
- Provide an opportunity for vendors to differentiate themselves from competitors
- Use the specifications to convey project requirements and gain clarity on vendor products
- Set evaluation criteria in alignment with the specifications or requirements

Establish written evaluation criteria. The evaluation criteria should reflect both the SOW and RFP specifications or requirements. The Evaluation Committee will use these criteria to compare vendors, offerings, price points, and non-price factors, and to select the best, most advantageous vendor. Most criteria are weighted and listed in priority order to indicate the importance of each specification. While price must be included as a factor, setting evaluation criteria that are price- and non-price-based allows the agency to select the proposal that is truly the best value. Well-documented evaluation criteria in alignment with project requirements are essential prior to the objective review, as the selection and award process will be more defensible.

Conduct a formal objective review process and document results. The RFP team should develop a written objective review process (known as an Objective Review Plan) to ensure the evaluation of proposals is done consistently and in accordance with a pre-approved process. The Objective Review Plan sets the criteria for review, rejection, selection, and award. An initial review of proposals will reject any failing to meet the mandatory requirements. Proposals that pass the initial review are then forwarded to the Evaluation Committee for review against evaluation criteria. After selection documentation is finalized, agencies communicate results to vendors.

Key Considerations

This phase should not be rushed—experts recommend at least 6 months and often up to 12 months, to develop an RFP, conduct an objective review process, and select a vendor. To avoid potential protests, project planners should understand and adhere to state and local procurement rules, establish evaluation criteria and an objective review process in advance of selection and award, and document evaluation outcomes in alignment with project requirements. If an RFP selection is contested, it could delay a project indefinitely.

Checklist: RFP and Acquisition Phase	
☐	**Develop a written action plan** – Identify members for an RFP team and establish roles and responsibilities – Set expectations for confidentiality – Understand procurement rules and timelines – Develop a clear understanding of services and products needed – Set milestones for the procurement schedule
☐	– **Form the RFP team,** including the Procurement Manager, Procurement Officer, General Counsel, Program Manager, Subject Matter Experts, and Evaluation Committee
☐	**Develop the Statement of Work (SOW)** in clear and concise language – Identify and incorporate minimum requirements – List basic services and products to be delivered
☐	**Include specifications or requirements in the RFP** – Identify minimum requirements for vendors – Ensure non-price requirements are provided at no additional cost – Include technical standards to ensure interoperability is established and maintained – Provide an opportunity for vendors to differentiate themselves – Confirm the SOW and the RFP specifications or requirements are consistent – Use specifications to convey project requirements and gain clarity on vendor products – Set evaluation criteria in alignment with the specifications or requirements – Ensure requirements meet user needs specified in Pre-Planning and Project Planning Phases
☐	**Establish written evaluation criteria,** well before the award – Align criteria to user needs, SOW, and RFP requirements – Assign weight to every criterion – Categorize the criteria in priority order and by evaluation weight (priority) – Develop an Objective Review Plan that includes evaluation criteria and selection factors
☐	**Conduct a formal objective review process and document results** – Conduct an initial review to reject proposals that don't meet minimum requirements – Document the objective review process and outcomes – Ensure all team members adhere to confidentiality agreements, procurement rules, and the formal objective review process as written – Communicate results to vendors based on evaluation criteria and selection factors

During the fourth phase, implementation activities occur after the system has been purchased. The goals of the Implementation Phase are to: develop an implementation plan; install and test new systems or components; transition or cut-over to new systems; update operational procedures and train users; and promote new communications capabilities and benefits to the community. There are often hidden costs and financial considerations during implementation. Project planners should identify residual costs and develop an implementation plan to cover those costs and ensure successful migration to new systems or components.

Recommendations

The following recommendations should be considered during the Implementation Phase:

Develop an implementation plan. Implementation plans (also known as project plans) are often developed at the start of a project, with high-level tasks and dates. Plans are refined during the RFP process to convey expectation to vendors, and then further refined after the RFP process based on negotiations with the selected vendor. Given the time between the project start date and procurement, project planners should ensure implementation plans—dates, milestones, roles, and responsibilities—are accurate and achievable. Project planners should coordinate with vendors to validate plans, as well as gain buy-in from senior officials and decision-makers on any revisions to ensure everyone understands the implementation process. Final implementation plans should include:

- List of tasks (e.g., install new system, test the system, train users, cut-over)
- Percentage completed (tied to status completion)
- Status of each task (which will change over time)
- Task start date (or planned start date) and end date (or planned end date)
- Completion dates
- Task owners
- Milestones (e.g., significant stage in project development, budget progress at key stages)

Experienced officials recommend including project- and budget-focused milestones in an implementation plan. While most project planners incorporate project milestones, many do not set budget milestones (e.g., targets for spending funds) in the same way. Budget milestones help planners monitor the percentage of funds spent to facilitate better monitoring and reporting, which is important for grant funds. Budget milestones also serve as progress indicators and keep agencies on schedule, especially in cases where funding expires (e.g., grant period of performance). Projected spending plans may also be required. Depending on the scale of the project cost as compared to the agency's budget, cashflow planning may be necessary.

Understand and document testing procedures in coordination with the Technical Committee. The *Lifecycle Guide* provides recommendations for the vendor and Technical Committee to fully understand testing criteria, procedures, and any dependencies, including costs. Testing procedures should be tied closely to an Acceptance Test Plan (ATP) that tests requirements

included in the FRD and RFP. The Association of Public-Safety Communications Officials (APCO) International[9] describes the testing process in greater detail, including:

Factory testing is performed on each piece of equipment at the manufacturer location. Vendors provide performance specification sheets on each piece of equipment, which should be retained by the project managers. Project planners should request that vendors provide documentation of compliance for equipment purchased (e.g., Project 25 standards for LMR). The document not only ensures equipment is standards-based, it also provides proof of compliance in the event the agency is audited by the granting agency, if grant funds were used to procure equipment.

Staging is the testing of a system at a factory or on-site. The *Lifecycle Guide* notes the vendor will often pass on costs associated with staging to its customer, whether it is in a factory or in the actual location to be installed. Agencies should understand what the vendor is offering and the associated costs. Neither factory staging nor on-site staging is simple or all-encompassing. Staging provides an opportunity to demonstrate the functions and features of the new system in a controlled setting. It also provides an opportunity to test equipment and conduct interoperability testing with third-party (or existing) equipment. Agencies need to understand the costs of staging (e.g., personnel needed to oversee demonstrations, travel to staging site) and build those costs into project plans and budgets.

BEST PRACTICE
Some agencies have saved costs by using in-house staff to install equipment and conduct site and coverage verification with vendors to test system performance.

Site acceptance occurs when the equipment is installed and tested on-site, site-by-site, to ensure equipment for the site is working. The purpose is to validate system operation. Some agencies have adopted a hybrid approach to site acceptance, where they install some equipment using in-house staff, and then work with vendors to test new equipment and interoperability with existing equipment. This ensures all equipment at an individual site is installed properly and operates as expected and allows the agency to save on installation costs.

Coverage verification occurs after all equipment is installed, tested, and accepted. The purpose is to measure the actual transmission of the new system against existing coverage and contractual expectations. Changes to equipment could yield changes to coverage, which then affect the coverage guaranty. Agencies should be aware there are significant costs to performing coverage testing. Roles and responsibilities for coverage testing should be carefully negotiated and defined in the final contract for the project. Lastly, agencies should document coverage and consider how the actual performance may affect the vendor's performance guaranty and other terms.

[9] See APCO International website for resources at: apcointl.org.

Testing/acceptance includes additional testing of the system as a whole once all sites are installed. The purpose is to test the system after installation, including its features and functions, as well as any sub-systems that have been integrated into the new system. Equipment, network performance, interoperability, and "failure scenarios" are all tested to simulate real-world operations. Agencies should ensure this is not simply an equipment check; rather, this should be a test against the functional requirements defined in the RFP. Agencies should be aware of additional costs during the testing period, including technical personnel who understand the functional requirements and can validate performance; backfill for personnel engaged in testing; and personnel who can make technical adjustments to agreements, legal documents, licenses, and guarantees as a result of changes to system performance or coverage.

BEST PRACTICE
Agencies should account for additional costs needed during testing, including technical personnel to oversee vendor testing, backfill for those technical staff, and personnel to modify any vendor agreements or other documents.

Cut-over is the transition period when agencies are testing new systems and troubleshooting issues. Whether a new system is more of a moderate upgrade or a system overhaul, a cut-over plan is necessary. Considerations include the cost of potential down time, the time of year to cut-over (e.g., tourist or hurricane season), how to communicate when the prime system is down, and interoperability considerations. Vendors typically offer assistance during this time, although the amount of time may vary. Agencies report a 90-day period is necessary to ensure a smooth transition from legacy to new systems as well as having a detailed cut-over plan. There are additional costs in this phase as well, including personnel to maintain legacy systems while new systems are coming online; training personnel to use new equipment; training technicians to identify and troubleshoot issues; and providing backup communications. Agencies should address all operator training requirements to ensure issues with the system cannot be attributed to operator error. Agencies should also maintain current (legacy) systems until the new system has been fully implemented and embraced by users.

BEST PRACTICE
Agencies should plan for the time and funding needed for training (including staffing and backfill costs). Training should be delivered "just in time" or simultaneous to the system roll-out.

Final acceptance occurs after all deficiencies in the system are addressed. Acceptance of the system indicates all functional requirements defined in the RFP are met, and the system performs to the required contractual specifications. A final ATP (FATP) should be developed and followed to ensure formal acceptace. 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.

BEST PRACTICE
Agencies recommended discussing with vendors the expected maintenance and operation costs, levels of support over time, and anticipated system end-of-life, so the agency can prepare its needs and messages to officials.

Experienced officials recommend tying the warranty to final acceptance, not at cut-over. Vendors will often assist as needed during the implementation phase to ensure the system is functional. The *Lifecycle Guide* recommends agencies tie warranties to the date when they

assume full responsibility for the system after final acceptance. This will maximize the length and value of the warranty.

Update operational procedures and train users. Agencies should ensure plans and standard operating procedures that include new communications capabilities and provide ongoing training to system users. Experienced officials recommend training and exercising to help response personnel understand their communications roles and responsiblities during an emergency, as well as the process for working with other agencies. As communications technologies continue to evolve, the need for training and exercises becomes even greater to ensure that personnel are proficient in using existing and new technologies. Agencies should involve responders from all levels of government, as well as non-governmental stakeholders, to practice a whole community response and identify gaps and problems with technologies or protocols. Continued investments in operational procedures, training, and exercises are needed to address gaps identified in response and recovery operations, which should include thoroughly testing resiliency and continuity of communications.

- *Normal Operations* are referred to as day-to-day operations and require a simple effective set of procedures that can be easily supported in the field.
- *Backup Operations* are a result of a component or system failure. System operating procedures should be established to support backup operations and tie back to the Continuity of Operations.
- *Emergency Operations* include declared (and instant) operational emergencies such as natural or manmade disasters.
- *Regional Operations* 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.

Promote new communications capabilities and benefits to the community. Once the system is operational, agencies should communicate the benefits to elected officials, funders, public safety users, and the whole community—especially if the project was supported with public funds, a special tax, or revenue bonds. Continuous training and promotion of the new system results in well-educated officials and users who appreciate the system's impact, which helps ensure future support. Experienced officials recommend providing annual reports to elected officials on the communications system's performance and needs. This has proven to be an effective means to communicate funding for maintenance, operations, replacements, and repair.

Key Considerations

Implementation of communications systems often takes 18 to 24 months to complete. It is important to understand the anticipated lifespans of system components during implementation, so agencies can plan the next phases of the lifecycle. Manufacturers and vendors are eager to develop the next generation of equipment. This results in shortened useful life of many legacy systems, especially as replacement parts and the support needed to maintain legacy systems are no longer available. Agencies should verify the level of support vendors provide during scheduled maintenance and possible support available beyond the warranty or maintenance agreements.

Checklist: Implementation Phase	
☐	**Develop the implementation plan, including:** – List of tasks (e.g., install new system, test the system, train users, cut-over) and owners. – Percentage completed and current status of each task – Task start/end dates and completion date (planned or actual) – Project- and budget- focused milestones – Risk (e.g., issues that have not occurred but are at-risk of occurring) and issues trackers (e.g., issues that have occurred and are being addressed by mitigation plans)
☐	**Understand and document testing procedures in coordination with the Technical Committee:** Factory testing – Request and retain documentation of factory testing Staging – Compare costs associated with off-site or on-site staging/testing – Choose off-site or on-site staging – Understand residual costs during staging (e.g., personnel, backfill, travel) – Assess staging performance/results Site installation and testing – Seek out cost-saving methods on installation and testing – Understand the proposed schedule for site installation and testing – Oversee the vendor during site installation and testing Coverage verification – Understand coverage requirements in the RFP – Assess and verify coverage analysis – Ensure changes to the system do not affect vendor warrantees and guarantees – Adjust agreements as necessary to reflect coverage changes Testing and acceptance – Discuss residual costs and ensure they are funded (e.g., technical staff, backfill, training) – Conduct vendor testing of entire system after installation – Engage stakeholders and end users to identify issues early – Ensure all system components, equipment, and features are functioning – Integrate sub-systems into the new system – Test network performance, interoperability, and failure scenarios – Record results and compare to requirements in the RFP – Address any deficiencies Cut-over – Develop a cut-over plan – Ensure residual costs are considered/funded (e.g., personnel, training, technical assistance) – Train operators to avoid attributing system errors – Confirm legacy and backup communications are available Final acceptance – Engage the Procurement Officer – Discuss expected lifecycle, ongoing costs, and refreshment options with the vendor – Retain vendor to provide initial support – Initiate the warranty

Checklist: Implementation Phase	
☐	**Update operational procedures and train users** to include new communications capabilities – Ensure proficient personnel through ongoing training and exercising across the whole community – Address gaps identified in response and recovery operations, testing resiliency and continuity
☐	**Promote new communications capabilities and benefits to the community,** including: – Project successes to users, elected officials, and citizens – Future funding needs to officials – Continued need for training to users

PHASE 5: SUPPORT, MAINTENANCE, AND SUSTAINMENT | YEAR 1 – YEAR 25

Once an emergency communications system has been installed, tested, and accepted, the public safety agency enters the Support, Maintenance, and Sustainment phase. The goals of this phase are to maintain the system and equipment, manage the budget, and continually assess and communicate needs to ensure the accepted system stays at optimal operational level during its life.

Experienced officials caution that communications system maintenance is complex. Agencies must manage many moving parts, including day-to-day operations; ongoing maintenance and repair of equipment, hardware, and software upgrades[10]; and asset tracking. In addition, systems and system components have varying lifecycle lengths, such as infrastructure, 20-25 years), fixed station equipment for example, 11-15 years), and devices for example, 3-4 years) as shown in **Figure 3**. To further complicate maintenance activities, agencies are typically managing multiple systems for example, LMR, data, IP-based broadband, alerts and warnings, and cybersecurity systems), while simultaneously planning for future capabilities or integration of systems for example, statewide or regional systems, FirstNet). Agencies must communicate system lifecycles and funding needs, as any delayed maintenance could have a negative impact on communications capabilities and response operations.

[10] New communications equipment often has computer-based elements (e.g., programmable radios, ability to interface with a computer, ability to interconnect with other components). These features and functions are helpful to communications managers but come with an additional cost. Software is continually being upgraded and new features and protections added; in turn, equipment with that software needs to be upgraded with the latest versions as they are released to ensure security features are installed and the equipment is compatible with other similar equipment.

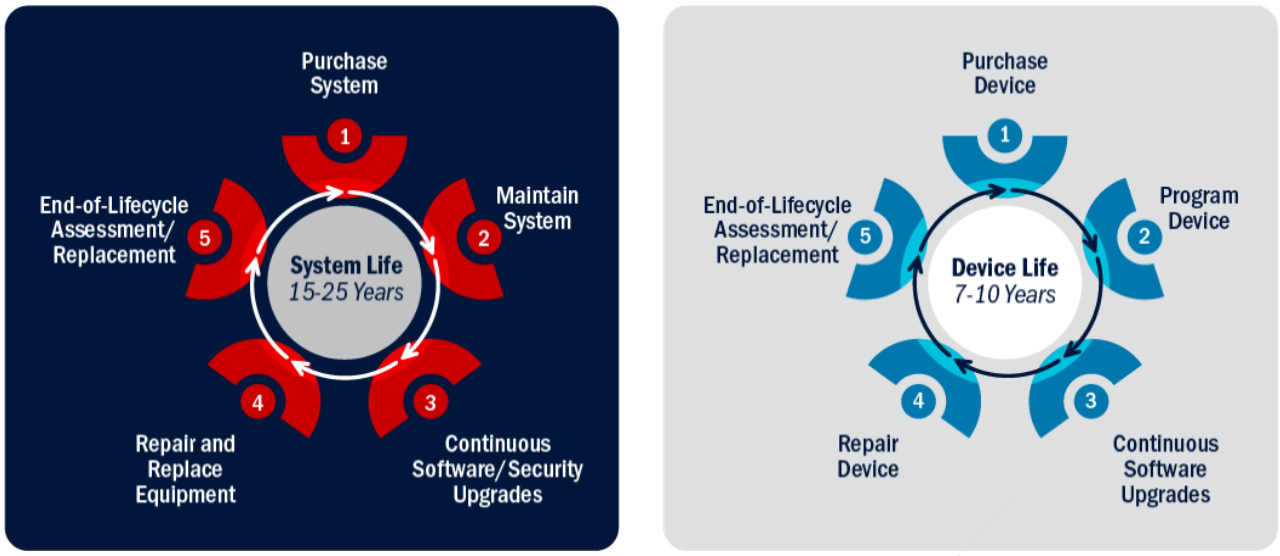


Figure 3: System and Device Lifecycles

Recommendations

The following recommendations should be considered during the Support, Maintenance, and Sustainment phase:

Maintain an accurate inventory of equipment. Inventorying communications equipment is an immense task. It is critical public safety agencies know where every piece of equipment is located, its capabilities, condition, and other factors for emergency preparedness. An accurate inventory assists countless maintenance tasks, such as reprogramming, servicing, updating, planning for regional and statewide interoperability, disabling lost equipment, grant reporting, and audits. It also provides agency officials with a broad view of current communications equipment and capabilities and enables officials to recognize and communicate future needs to decision-makers.

The best time to start an inventorying system is when a public safety agency first takes ownership of assets. During the acceptance of new systems and equipment, vendors and procurement agents confirm delivery from the purchased list and provide a full accounting. Public safety agencies use this initial inventorying to build their own inventory list for all equipment, adding in location, tracking identification information, responsible agency, user information, and projected replacement dates,[11] among other asset inventory data elements. The following checklist identifies critical steps for planning and conducting an asset inventory.

Checklist: Asset Inventory	
☐	**Determine the inventory scope** (e.g., conduct an enterprise-wide inventory including all communications equipment, or update an existing inventory system)
☐	**Identify all data elements to collect and track;** APCO International recommends: – Agency: Department in possession of the radio

[11] There are several factors affecting replacement dates besides optimal lifespan of the equipment, including requirements or desire to migrate to a new technology; interoperability needs with a new or existing statewide or regional system; lack of replacement parts; and cost of maintenance or upgrades outweighing cost of purchasing new equipment. Experts report the rapid rate of technological changes and the expansion of integrated communications systems also impact decisions to replace equipment. Agencies must maintain awareness of the whole communications environment and set replacement dates based on their best understanding of needs.

Checklist: Asset Inventory	
	– Make: Manufacturer of the radio – Model Name: The manufacturer-assigned model name – Model #: The manufacturer-assigned model number – Serial #: The equipment's serial number – License #: There may be a need for a license # (for software) – Type: Control station, portable, mobile, etc. – Asset #: Your agency's asset number affiliated with the radio, if any – Band(s): VHF, UHF, 800 MHz, etc. – Condition: Create a consistent code to indicate the physical condition (e.g., simple 1-5 scale, with 1 meaning "This radio should be replaced" to 5 meaning "Like new condition") – LOC1: Primary location to which this piece of equipment is assigned – LOC2: Specific location where equipment is permanently mounted or stored when not in use – Channels: Number of channels in the radio (if applicable) – MFG date: Date of manufacture, as shown on a manufacturer's plate – Firmware version: Version number and date of radio's firmware – Radio ID: Push to talk or internal ID of radio – Alias: If an alias has been programmed for the radio, show it here – Program: If your agency uses standard templates to program your radios, indicate here (e.g., "EMS Supervisor") – Rebanded: Status of rebanding (if applicable) – Narrowband: Status of narrowband (if applicable) – Encryption capable: Yes or No – Encryption type: AES, DES-OFB, etc. – Encryption enabled: Yes or No – Purchase date: Date radio was purchased, if known – Purchase price: Price paid for initial purchase of radio, if known – Funding Source: Grant, state funds, etc. – Accessories: Holster, charger, speaker/mic, etc. either provided upon issuance or later – Last Inspected: Dates on which the equipment was last inspected – Last Upgraded: Dates on which the equipment/software was last upgraded – Upgrade Due: Dates on when the equipment is scheduled for upgrade (if applicable) – Notes: Free-form notes about the radio (e.g., repair notes, transfer notes) – Fleet information: some agencies keep a separate list for vehicles – FCC Licenses: Number and status of licenses
☐	**Determine and list sites for all inventory,** which may include fire/police stations, substations, dispatch centers, transmitter sites, satellite receiver sites, and other sites where assets are stored
☐	**Consider options and develop/purchase the inventory tool,** such as an Excel spreadsheet with drop-down boxes, or a Web-based tool enabling multiple agencies to update information online
☐	**Determine how data will be collected** (e.g., initial inventory list provided by vendor; automatically via radio test/diagnostic mode to provide serial number, firmware version, etc. through a key combination/cable connection to a laptop; manually during a physical examination of the equipment; or a combination of solutions)

Checklist: Asset Inventory	
☐	**Determine how equipment will be tracked and marked,** such as asset tags affixed to equipment corresponding to a number in asset inventory; bar codes; Quick Response codes; or color-coded stickers. For vehicle-installed equipment, consider how asset tags will be accessed when the vehicle is fully loaded with equipment
☐	**Determine the inventory team,** including personnel who are savvy about communications equipment
☐	**Prepare to collect information** – Distribute data elements to inventory team, solicit feedback, and update the tool as needed – Ensure laptops being used to collect data have the software needed to read equipment numbers and software versions are up-to-date – Coordinate with each site to schedule an inventory session; ensure all users have or bring all equipment to the inventory session – Schedule training for inventory team
☐	**Train and assign locations to the inventory team** – Train the inventory team on capturing data in the selected tool – Create a mechanism (feedback loop) to capture idiosyncrasies found while collecting data so team members are managing idiosyncrasies in the same way (i.e., standardized data collection) – Assign team members to specific locations – Provide targeted milestone and completion dates
☐	**Conduct the inventory** – Survey all equipment information and record into the inventory tool – Make note of missing information – Keep a list of departments/agencies that need to be revisited
☐	**Revisit departments/agencies to collect any missing information** – Prepare a list of missing information and send to specific departments/agencies – Revisit to collect missing information
☐	**Compile data** – Appoint a single person to review, assure, and compile data – Conduct quality assurance on data – Make a list of any remaining information to be tracked down – Indicate any caveats in the Notes section of the database – Record best practices and lessons learned
☐	**Develop processes for maintaining data** – Create policies and processes for updating inventory (e.g., reporting transfer or loss of equipment) – Distribute policies and processes to personnel – Remind personnel frequently of the importance of an accurate inventory

Once the inventory data has been collected, agencies should use the information to manage the maintenance of equipment, including:

- Identify equipment that needs immediate upgrades or replacement
- Plan future purchases (e.g., purchase equipment that has been most reliable, avoid equipment that required frequent repair)
- Estimate future budgets (e.g., request regular intervals of funding based on regularly occurring costs, estimate replacement timelines and budgets at the start of a new project)
- Communicate ongoing costs and needs to decision-makers based on real-time information
- Inform grant proposals and risk assessments
- Identify and prioritize equipment that can be purchased when funds become available
- Extend or amend service contracts

Determine and execute an ongoing Maintenance and & Operations (M&O) model. During the lifespan of a communications system, public safety agencies must actively maintain equipment from the start. There are different types and levels of support, including:

- System-level support activities—also referred to as operations—to ensure equipment is operating and functioning for example, managing software, access, outages, cyber incidents)
- Maintenance activities to fix anything broken or prevent something from failing
- User support for answering operational questions for example, helpdesk, radio shop)

BEST PRACTICES

- Continually assess equipment status for optimal operation
- Ensure equipment is functioning properly before the warranty period expires.
- Monitor M&O ticket items and repair requests managed by the vendor or the agency to inform future purchases (e.g., identify radios that are constantly in the shop or need to be repaired)
- Monitor repair costs as reported by the vendor or recorded by the agency (e.g., replacement parts, level of effort) to understand full cost of M&O program and to inform future decisions
- Continually communicate with the vendor on solutions available after M&O contracts have expired (e.g., will the vendor still support the system, will replacement parts be available)
- Stockpile spare parts while they are available (i.e., before the vendor stops supporting or discontinues manufacturing certain parts); this can significantly extend the lifespan of equipment
- Carefully monitor and install all software and security upgrades; failure to upgrade software can lead to system failure, compromise of security, system shut-down, or increased costs

Vendors typically provide **Initial Support** immediately after the system is installed. During this timeframe, the system and equipment are under warranty—guarantee on parts and installation—and include assistance with training, operations, and user support for a short period of time. Specific requirements are often detailed in the purchasing contract. Public safety agencies should request and compare warranty offerings from various RFP responses to:

- Make informed decisions during vendor selection processes
- Be in the best position to negotiate terms and conditions of contracts with vendors
- Save money—the longer the vendor is supporting the system, the less time agencies are providing support, which may yield significant cost savings
- Inform details on warranty conditions for future contracts

M&O requires long-term support, which can be provided by the vendor (at an additional cost), by in-house staff, by a third-party provider (e.g., another public agency or a private entity established through an Interagency Agreement [IAA] or contract), or through a combination of providers. Each model has its advantages and disadvantages. **Table 2** provides a comparison of these maintenance and operations models.

Table 2: Comparison of Maintenance and Operations Models

Models	Advantages	Disadvantages
Vendor, including parts and labor	• Vendors understand the system and often provide a fast solution to any issues • Agencies can learn from vendor solutions • Agencies are under obligation to pay per contract terms; thus, the level of service is not affected by fiscal climate	• This is typically the highest-cost option • Agencies have less control over the level of support and solution offered • Agencies may rely on vendors and not learn how to effectively operate the system or troubleshoot any issues
In-house staff	• This is typically the lowest-cost option • Agencies have the greatest control over the level of support and solutions • Agencies learn how to effectively operate the systems and troubleshoot any issues	• There is a steep learning curve for new systems • Staff may not have the technical ability • The level of maintenance can be affected by the agency's fiscal climate • There may be additional costs for parts and some labor
Third-party public agency	• There are typically high-quality technical staff • This allows for efficient operations and potential cost-savings across enterprise-wide operations • Knowledge is retained within the public agency	• This requires an IAA signed by leadership • The primary agency has less control over level of support and solutions offered • This may lead to over reliance on third-party technicians to fix issues and agency does not learn how to effectively operate the system • This may not include parts and labor costs

Models	Advantages	Disadvantages
Third-party private entity	• Typically high-quality technical staff • This is a good option if agency does not have knowledgeable staff to manage M&O	• This requires a separate service contract • This may lead to over reliance on third-party technicians • This may not include parts and labor costs

Agencies should select an M&O model based on their individual capacity, needs, and funding availability. Some agencies choose an approach during the Pre-Planning Phase as part of the project proposal or seek grant funds to support M&O costs.[12] Alternatively, other agencies wait until the RFP and Acquisition phase as vendors may offer a robust warranty or affordable M&O package with the purchase of the new system. Regardless of the timing of this decision, agencies should understand what the M&O provider is offering (e.g., warranty conditions, parts, labor, software upgrades, hardware repair, security upgrades).

Manage the budget. Agencies make several budget decisions prior to this phase, including:

- When the project is conceived, determining how capital and ongoing costs will be paid (e.g., bonds, general revenue, revenue from traffic tickets)
- During the evaluation of RFP responses, determining which vendor offers the optimal M&O package for the best value
- After the system is accepted, conducting an asset inventory and monitoring equipment status, repairs, costs, and replacement dates to estimate the lifespan and to plan future budgets

Knowing the manufacturing date, trends in repair, general maintenance costs, and estimated lifespan of equipment, agencies can budget for replacement before a failure occurs or before the manufacturer ends support. **Figure 4** provides a long-term budget that shows periodic replacement of equipment after an initial inventory assessment.

[12] Agencies should review grants to ensure M&O is an allowable cost and understand any restrictions. In some Department of Homeland Security (DHS) grants, maintenance contracts, warranties, repair or replacement costs, and upgrades may be allowed but there are restrictions on renewal contracts. Warranties purchased with the system can extend beyond the grant period of performance (e.g., agency can purchase a 5-year maintenance agreement even if the grant has a 2-year period of performance). However, after the initial purchase, the agency is not allowed to purchase a service agreement with grant funds extending beyond the grant period of performance.

This shows $55,000/year maintenance of portable and mobile radios, then major investments ($5.5M, $10.1M) in portable and mobile radios for years 6–10

This is a 15-year budget based on data collected through asset inventorying for a large statewide communications system

Year	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035	TOTAL
Replace Constellation/Eclipse	$0	$0	$0	$5.5M	$0	$0	$0	$0	$0	$0	$0	$0	$4.4M	$4.4M	$4.4M	$18,700,000
Replace Portable and Mobile Radios	$55K	$55K	$55K	$55K	$55K	$5.5M	$5.5M	$10.1M	$10.1M	$5.5M	$55K	$55K	$55K	$55K	$55K	$37,250,000
Replace Conventional VHF Repeaters	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$4.4M	$4.4M	$0	$0	$8,800,000
Replace Generators	$55K	$55K	$55K	$55K	$55K	$55K	$55K	$55K	$55K	$55K	$55K	$55K	$55K	$55K	$55K	$825,000
Replace MPLS Network	$27.5K	$27.5K	$27.5K	$27.5K	$27.5K	$27.5K	$2.2M	$5.5M	$27.5K	$27.5K	$27.5K	$27.5K	$27.5K	$27.5K	$27.5K	$8,057,500
Update Building and Towers	$0	$0	$0	$825K	$825K	$825K	$825K	$825K	$825K	$825K	$5.225M	$825K	$825K	$5.225M	$825K	$18,700,000
Replace Batteries	$275K	$275K	$275K	$275K	$275K	$275K	$550K	$550K	$550K	$550K	$550K	$550K	$550K	$550K	$550K	$6,600,000
Replace TRS Switch	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$2.75M	$0	$0	$0	$0	$2,750,000
Replace TRS Site Equipment	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$11.88M	$0	$11,880,000
Replace TRS Routers	$0	$0	$0	$0	$0	$0	$0	$1.265M	$0	$0	$0	$0	$0	$0	$0	$1,265,000
Replace Dispatch Consoles	$0	$0	$0	$0	$0	$0	$0	$0	$5.555M	$0	$0	$0	$0	$0	$0	$5,555,000
Plan Development	$0	$0	$0	$0	$0	$0	$0	$0	$825K	$825K	$825K	$0	$0	$0	$0	$2,475,000
Annual Totals	$412,500	$412,500	$412,500	$6,737,500	$1,237,500	$6,682,500	$9,130,000	$18,295,000	$17,937,500	$7,782,500	$9,487,500	$5,912,500	$10,312,500	$22,192,500	$5,912,500	$122,857,500

This shows $0 investment in towers for at least 3 years, then significant investments ($825,000+/year) in years 4–10. The replacement/rebuild costs for years 11 and 14 increased to $5.225M

This shows that some equipment (e.g., TRS switch, routers, dispatch consoles) needs to be replaced only once during the 15-year period

Costs for plan development vary depending on organization, system size, and whether in-house or contracted services need to plan for system replacement

This shows an increased investment of $550,000 for anticipated replacement of older batteries

Figure 4: Sample Lifecycle Plan and Budget

This sample budget includes all components of a communications system, information on current state, maintenance costs, and insight into replacement dates. For example, some equipment requires no immediate investment; some equipment requires steady, ongoing funding; some equipment needs to be replaced only once; and other equipment is so mammoth and costly that funding is spread across several years. Estimated costs will vary by system configuration, staff, and other resources. The sample budget includes:

- Ongoing costs (e.g., $55,000/year for generators)
- Major capital investments and estimated dates (e.g., $11.8M for new site equipment in 14 years)
- Total funding needed each year and overall

Share communications needs with decision-makers early and continually. Experts report as complex as system support, maintenance, and sustainment can be it may be as challenging to educate decision-makers about ongoing emergency communications costs. Agencies should coordinate with statewide and regional communications leaders, governing bodies, and elected officials, as well as prepare an annual report to convey ongoing communications system needs and costs. The key messages public safety agencies must communicate include:

- **Communications systems are not a one-time investment.** Systems require a large initial capital investment, as well as ongoing funding for upgrades, repairs, replacement, and operations (e.g., fuel for generators). Agencies should communicate ongoing needs from the start and should continually share long-term budget projections to educate elected officials and decision-makers on anticipated costs (e.g., ongoing, short-term, long-term) of communications systems.
- **Systems are comprised of a variety of interconnected components, each with their own optimal lifespan.** Agencies should overlay their long-term budget projections to show interval replacement dates and investments required over time, so components are replaced on time or as needed to keep the system operating. While some system components need infrequent M&O, other components may require extensive repairs, reprogramming, or replacement (e.g., portable equipment) to maintain communications.
- **Technicians are managing multiple lifecycles simultaneously.** For example, an agency may be managing a 20-year infrastructure lifecycle, an 11 to 15-year fixed station equipment lifecycle, a 10-year mobile equipment lifecycle, and a 7-year portable equipment lifecycle, at the same time it is planning to migrate toward a statewide or regional system. Agencies should explain how current communications systems must be sustained prior to migrating to new communications capabilities, meaning M&O costs will continue through the End-of-Lifecycle Assessment and Replacement phase.

Key Considerations

This phase spans from the moment the system becomes operational until transition to its replacement—sometimes 25 years or more in traditional LMR systems. Agencies should employ these best practices to understand the budget requirements and raise awareness of M&O needs. A key take-away is that a communications system is only as good as the ability to keep it running. Maintaining a system can be difficult and costly, but public safety agencies cannot afford to be without a sound maintenance plan.

Checklist: Support, Maintenance, and Sustainment Phase	
☐	**Maintain an accurate inventory of equipment,** through enforcement and reminders of asset inventorying policies and requirements
☐	**Determine and execute an ongoing M&O model,** in consideration of the agency's needs, staffing ability, and funding. M&O may be provided by the vendor, by in-house staff, by a third-party provider (e.g., another public agency or private entity), or through a combination of providers
☐	**Upgrade hardware and software, as needed,** to avoid negative impacts to operations, compatibility with partner agencies, security, access, and functionality of equipment
☐	**Manage the budget** and build M&O expenses and personnel to effectively manage system assets (e.g., continually monitor asset inventory) into plans from the start – Report any unexpected costs to project managers immediately
☐	**Share emergency communications needs with decision-makers early and continually** – Coordinate with the SWIC, SIGB/SIEC (if necessary or required), state and local officials, state planners, SAA, risk managers, and users to convey ongoing communications system needs and costs – Prepare an annual report and brief state/local legislature regularly on the status of the communications system and funding priorities

PHASE 6: END-OF-LIFECYCLE ASSESSMENT AND REPLACEMENT | YEAR 7 – YEAR 25

Previously titled the Refreshment step, the *Lifecycle Guide* provides guidance on assessment and refreshment activities to ensure the system continues to support users' needs over the system's useful life. Technology refreshment does not necessarily mean system replacement. Refreshment includes the infusion of technology advancements and accommodation of new standards or operational needs, including new interoperability requirements. However, at some point in time, a system will reach its end-of-life and need to be replaced. The goals of this phase are to conduct ongoing assessments of current systems, refresh or upgrade systems as needed to extend the life of the systems, and determine when to replace the system or system components with the solution to best fit an agency's operational and technical needs.

Recommendations

The following recommendations should be considered during the End-of-Lifecycle Assessment and Replacement phase:

Conduct ongoing assessments of current systems. Assessments involve tracking operational suitability, stability, and potential failure points, as well as conducting an overall cost analysis to account for capital expenditures, recurring costs, and maintenance. Project planners should facilitate periodic meetings with end-users to provide insight into current communications capabilities and gaps, and to identify key performance indicators to signal when the system nears

the end of its useful life. When considering capabilities or features, agencies must analyze benefits, costs, and potential impacts of future demographic and operating environment shifts, including expansion of services, workforce, and areas of operation. To assist in assessment, agencies may implement a balanced scorecard to plan for technology maturity:

Implement a balanced scorecard to plan for technology maturity. A balanced scorecard refers to a performance management report used by project planners to capture relevant information for managing the implementation of a strategy or operational activities. Following data collection with system technicians, users, and stakeholders, project planners should develop a balanced scorecard as a quick assessment of the public safety mission critical systems in use. The balanced scorecard provides a forward-thinking approach towards technologies that advertise a migration strategy with minimal stranded system exposure. As part of the ongoing lifecycle planning and review, project planners should also include the state of technology in use and emerging technologies.

Refresh or upgrade systems as needed to extend the life of the systems. Project planners should review possible technologies to extend the life of mission critical communications systems. Similar to aspects of conventional computer systems, many of the features, enhancements, and newer developments of communications capabilities are reliant on periodic upgrades of the operating systems and cybersecurity protections. Version upgrades – to hardware and software – are often sequential and require the installation of all intermediary version upgrades; thus, it is imperative that agencies install upgrades in a timely manner to avoid extensive costs, potential downtimes, and unnecessary exposure to security threats.

Determine potential replacement solutions. When determining the appropriate end-of-life of current systems and evaluating new technological replacements, project planners should consider the following:

Support national, state, and regional interoperability initiatives.[13] Interoperability has evolved over the years and is a necessity for public safety communications, rather than only a consideration. As replacement solutions are considered, project planners should understand what interoperability efforts are underway which may impact system design or advancements. Agencies are migrating to regional initiatives and statewide communications systems, as well as gateway approaches that link regional and local systems via the "systems of systems" approach. Project planners should coordinate with area leaders and governing bodies to support and align with national, state, and regional interoperability initiatives.

Consider early adoption of new technologies. Technical innovation provides opportunities previously unavailable. The rate of technical innovation is increasing exponentially. 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, and be prepared to analyze the full cost/benefit of these features. The innovation adoption lifecycle, as shown in **Figure 5**, is a visual representation of the times agencies tend to adopt new technologies. *Innovators* make up 2.5% of the population and are

[13] CISA leads the Nation's operable and interoperable public safety and national security and emergency preparedness communication efforts. The office collaborates with stakeholder groups such as SAFECOM and NCSWIC to develop policy guidance (e.g., *National Emergency Communications Plan, SAFECOM Guidance on Emergency Communications Grants*), and offers technical assistance to help federal, state, local, tribal, and territorial governments improve emergency communications.

the group to be the first to adopt an innovation. *Early adopters* make up 13.5% and are the second group of individuals who will adopt an innovation. The *early majority* consists of 34% of the population. This group will adopt a new technology over a varying amount of time and after confirmation of reliability of the innovation. *Late majority* is also 34% of the population and due to their skepticism, they wait until a majority of society has adopted the innovation. *Laggards* are at the end of the innovation adoption lifecycle, making up 16% of the population, and are the last to adopt an innovation, typically due to financial reasons or restrictions.

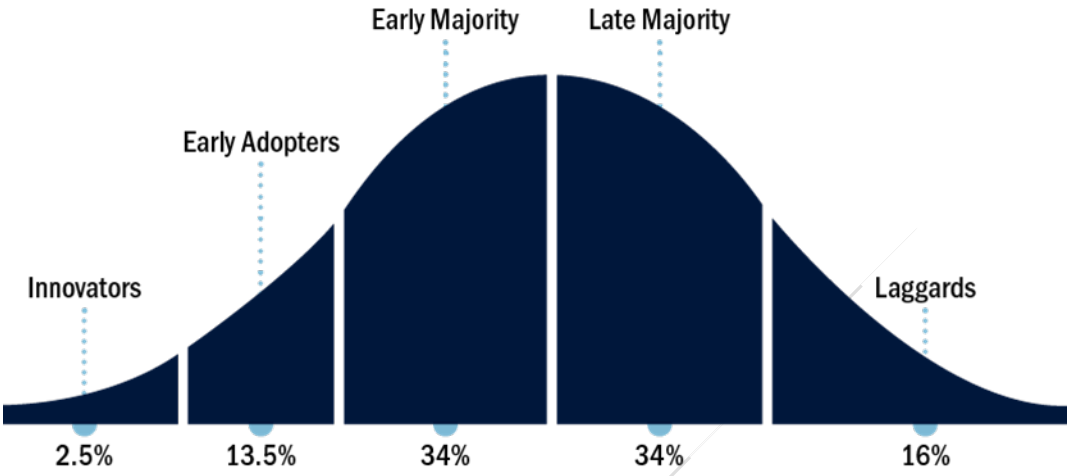


Figure 5: Innovation Adoption Lifecycle

Public safety mission critical communications systems have stringent survivability requirements, which makes early technology adoption difficult. Project planners should consider the environment in which public safety users operate and why, for a variety of reasons, they are not usually the first to adopt new technology. The risk of jumping in too soon is significant, while tried and tested solutions may be a more reliable model. It is important to understand the potential impacts before investing. However, there are certainly new technologies for which public safety agencies can, and should, be the innovators, and consideration should be given to adopting these technologies to improve response and recovery when the risk to the mission critical nature of the system can be identified and managed. It is important to look toward technologies that advertise a forward migration strategy with minimal stranded system exposure.

Adhere to widely used technical standards. Adoption of technical standards promotes interoperability and provides protection from isolation and obsolescence. For example, experts recognize the Project 25 (P25) suite of standards for the design and manufacture of interoperable, digital two-way wireless communications products for LMR systems.[14] Agencies should adhere to technical standards for all communications technologies (e.g., long-term evolution [LTE] for broadband/IP-based systems, Common Alerting Protocol for alert and warning systems). Reference the *SAFECOM Guidance on Emergency Communications Grants* and various products from the Federal Partnership for Interoperable Communications for additional information on technical standards relevant to public safety communications

[14] To learn more about P25 standards, visit the P25 Technology Interest Group website at: project25.org.

systems. While technology is not the sole component of ensuring interoperable communications, it is a major facilitator of interoperability, and standards help make it work.

Key Considerations

Continual assessments will occur throughout the system lifespan to identify any gaps or areas for refreshment. As the system ages and nears its end-of-life, agencies should circle back to Pre-Planning phase activities to determine replacement solutions, gain leadership approval, and solidify funding support.

Checklist: End-of-Lifecycle Assessment and Replacement Phase	
☐	**Conduct ongoing assessments of current systems** – Meet with users to determine the status of communications capabilities – Assess operational suitability and stability – Identify system weaknesses, both technical and operational – Analyze system expenses including capital expenditures, recurring costs, and maintenance – Review the potential impacts of future demographic and operating environment shifts, including expansion of services, workforce, and areas of operation – Implement a balanced scorecard to plan for technology maturity
☐	**Refresh or upgrade systems as needed to extend the life of the systems** – Review possible technologies to extend the life of mission critical communications systems – Upgrade hardware and install software versions to maintain operations and security
☐	**Determine potential replacement solutions**, with considerations to: – Support national, state, and regional interoperability initiatives – Consider early adoption of new technologies – Adhere to widely-used technical standards; reference the *SAFECOM Guidance on Emergency Communications Grants* and products from the Federal Partnership for Interoperable Communications

PHASE 7: DISPOSITION | 90 DAYS AFTER CUT-OVER OR TRANSITION

Disposition is the final phase in the *Lifecycle Guide*. System asset disposal is often the least considered step during system lifecycle planning. The goals of the Disposition phase are to weigh the options for disposal, dispose of the old system or system components in accordance with legal limitations and business requirements, and ensure minimal impact to operations of the new or upgraded system.

Although disposition of a communications system occurs at the end of the lifecycle, disposition planning should begin as early as the Pre-Planning phase. Depending on the system and its components, there may be many disposition options available or very few. Ideally, disposition of equipment should occur within 90 days after agencies transition to new systems. Considering available

options and coordinating with partner agencies early will help to ensure potential recipients have time to explore whether the offered components meet their needs and are compatible with their system. As an added incentive to early disposition planning, public safety agencies may benefit from demonstrating how savings or contribution to support a partner agency's need partially offsets investment in a new or upgraded communications system.

Recommendations

The following recommendations should be considered during the Disposition phase:

Reuse old components in the new system. Project planners should consider the entire system and possible reuse of equipment, along with a review of the risk management strategy that addresses system failure points and backup plans. Before disposing of equipment, review whether components may prove valuable as backup or secondary communications pathways. Those making these considerations should weigh the benefits of incorporating older components against potential risks posed to the new system while maintaining operability and interoperability.

Repurpose old components to another department. Project planners should also consider repurposing system components to another public safety agency regardless of jurisdictional boundaries, if allowed. The receiving department or unit may be able to use the components to support their operations or create a new communication capability. Use of refurbished and repurposed equipment often occurs out of necessity as a stopgap solution for agencies that do not have sufficient funding for new upgrades. In effect, repurposing old components stretches the budget for communications equipment that is approaching or at its end-of-life by adding time until complete replacement or upgrade is necessary. An evaluation of the condition and usefulness of the equipment should be included in the plan to make sure the donation meets the needs of the receiving department or agency.

Consider space availability. Project planners should understand space requirements, such as the physical size of equipment shelters, antenna loading on towers, power capacity, and heating and cooling systems necessary to support legacy and new systems during the transition. As a result, installations may be subject to tight quarters during the initial migration while multiple systems are operational. Project planners should also consider space freed by unnecessary equipment and plan for its removal—the timeframe for dual operations of old and new components within the transition plan is crucial. Space considerations may be short-term during the system migration or long-term depending on how planners determine to reuse or dispose of old components.

BEST PRACTICE

Adopting excess equipment from larger agencies remains a popular tactic among smaller agencies. While vendors may offer small trade-in value for used equipment when procuring new systems, it typically provides minimal financial impact to donor agencies. Instead, agencies can assist partner agencies when upgrading their systems and capabilities.

Convey surplus property to partner agencies. Surplus property refers to equipment not compatible with the new system, but all or part may be useful to another department or agency. Prior to announcing the availability of surplus property to partner agencies, there should be a clear understanding by giving and receiving agencies of statutes and policies related to surplus exchange. Both sides should obtain approval at the appropriate level prior to action. If grant funds were used to obtain the equipment, disposition of the property must conform to grant requirements, if necessary.

Document depreciation. It is important to manage property by expectant life versus financial value. All agencies must answer to an accounting entity; therefore, addressing the usable life of the equipment in light of any pre-existing amortization schedule will streamline the process. If the old system or equipment was classified as capital, it is essential to document the disposition of the assets so it can be fully depreciated.

Key Considerations

The disposal of systems and system components requires thoughtful consideration to ensure compliance with statutes, Executive Orders, and policies, as well as business requirements of the jurisdictions disposing of and receiving the property. Use of refurbished and repurposed equipment requires appropriate protocols, effective oversight, and adherence to established technical standards (e.g., P25 for LMR, LTE for broadband/IP-based systems). In addition, property purchased with the assistance of grant funds must be disposed of in compliance with any grant requirements. Repurposing or donating system components and equipment may create or improve communication capabilities. Project planners must consider all advantages and disadvantages prior to disposal.

Checklist: Disposition Phase	
☐	**Develop a disposition plan** – Incorporate disposition planning early in the project planning process – Review past projects to learn how long the Disposition Phase has taken for similar projects – Build sufficient time for planning into project work plans
☐	**Engage stakeholders and partners early to understand user needs and requirements** – Convene a meeting with disposition leadership, managers, and appropriate team members – Discuss activities in the disposition plan and assign leads to relevant activities – Determine how users and user needs may affect project disposition and the timeline
☐	**Identify disposition options in consideration of legal limitations and business requirements** – Reuse old components for the new system – Repurpose old components into another department – Consider space availability for equipment – Convey surplus property to partner agencies regardless of jurisdictional boundaries
☐	**Brief leaders on disposition plans** – Obtain final, formal approvals on the disposition plans – Consider rolling unresolved issues and changes into the next phase of a new project – Communicate user needs to elected officials – Share results with relevant stakeholder bodies (e.g., Statewide Interoperability Governing Bodies, Regional Emergency Communications Coordination Working Group)
☐	**Identify lessons learned following disposition** – Ensure compliance with funding closeout requirements, if applicable – Conduct a post-disposition survey or session to solicit feedback with stakeholders – Compile a closeout report showing final status of system issues, changes, risks, and costs – Share lessons learned with stakeholders and officials to assist with future decision-making – Reassign remaining disposition staff to other assignments

Conclusion

Public safety officials make numerous decisions to fund, plan, procure, implement, support, and maintain communications systems, and eventually replace and dispose of system components. This continuous system lifecycle planning can be daunting. To assist officials, this *Emergency Communications System Lifecycle Planning Guide* is intended to provide considerations and recommended actions through easy-to-use checklists for each phase of the system lifecycle planning model. These checklists combine best practices and lessons learned by public safety officials and experts who have successfully managed communications systems across the nation—from initial planning through final disposition. Agencies may contact CISA, SAFECOM, and NCSWIC with questions on this document or requests for assistance.

About SAFECOM/NCSWIC

SAFECOM is comprised of more than 85 members representing federal, state, local, and tribal emergency responders, and major intergovernmental and national public safety associations, who aim to improve multi-jurisdictional and intergovernmental communications interoperability through collaboration with emergency responders and policymakers across federal, state, local, tribal, territorial, and international partners. SAFECOM members bring years of experience with emergency communications during day-to-day operations, and natural and man-made disasters. SAFECOM members offer insights and lessons learned on governance, planning, training, exercises, and technologies, including knowledge of equipment standards, requirements, and use. SAFECOM members also provide input on the challenges, needs, and best practices of emergency communications, and work in coordination with CISA to share best practices and lessons learned with others.

NCSWIC is comprised of Statewide Interoperability Coordinators and their staff from the 56 states and territories. NCSWIC assists states and territories with promoting the critical importance of interoperable communications and sharing best practices to ensure the highest level of interoperable communications within and across states and with their international partners along the borders.

The Joint SAFECOM and NCSWIC Funding and Sustainment Committee developed this document with support from CISA. This document reflects the expertise and knowledge of SAFECOM and NCSWIC members, and the coordination efforts of CISA in bringing stakeholders together to share technical information, best practices, and lessons learned in funding and deploying public safety communications systems. Questions on this document can be sent to: SAFECOMGovernance@mail.cisa.dhs.gov and NCSWICGovernance@mail.cisa.dhs.gov.

Appendix: Definitions

Sources: Many of the terms listed below were pulled 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* (search.org/files/pdf/TECHGUIDE.pdf)
- COPS Office – *Law Enforcement Tech Guide for Communications Interoperability: A Guide for Interagency Communications Projects*, 2013 (search.org/files/pdf/LawEnforcementTechGuide_CommunicationsInteroperability_2013_508C.pdf)
- CISA – *National Emergency Communications Plan* (NECP), (cisa.gov/national-emergency-communications-plan)

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.

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 responsiblities.

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.

Gateway (COPS Law Enforcement Interop Guide)

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

Interoperability (NECP)

Ability of emergency response providers and relevant government officials to communicate across jurisdictions, disciplines, and levels of government as needed and as authorized.

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.

National Emergency Communications Plan (NECP)

The Homeland Security Act of 2002, as amended, requires CISA to develop the NECP; the NECP serves as the nation's strategic plan for improving emergency response communications and efforts in the United States.

Project manager (COPS Law Enforcement Tech Guide)

An individual dedicated to, and accountable for, all project-related activities and who is soley 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 (NECP)

A system designed specifically to meet public safety needs 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.

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 (NECP)

Generally refers to a reference document or an operations manual that provides the purpose, authorities, duration, and details for the preferred method of performing a single function or a number of interrelated functions in a uniform manner.

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.

Technical Committee (COPS Law Enforcment 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.