SAFECOM® NCSWIC®

Funding and Sustaining Land Mobile Radio (LMR) Trio

Part 3: Educating Project and Acquisition Managers on Project 25

Introduction

Public safety agencies use land mobile radio (LMR) systems as the primary means for transmitting mission-critical voice communications and low-speed data between public safety responders. As LMR systems and technologies have evolved over many decades, there are a variety of communications systems in use today. Traditionally, systems are designed to meet specific agency missions and operate on assigned frequencies/channels within appropriate spectrum bands (e.g., very high frequency [VHF], ultra-high frequency [UHF], 700 megahertz [MHz], 800 MHz). Vendors built LMR systems and equipment that were non-standard, and offered vendor-specific features that could inhibit interoperability with surrounding systems and equipment. As a result, disparate LMR systems emerged and were not always compatible with each other, making it difficult for public safety officials to communicate across jurisdictions and disciplines. Public safety recognized a need to standardize systems and equipment to ensure that responders could communicate regardless of system or vendor.

As digital protocols and trunking technologies were introduced in the late 1980s and early 1990s, the public safety community and federal government recognized the need for standards to enhance communications interoperability, while maintaining a competitive marketplace for public safety agencies.

Developing Standards

The federal government, in partnership with the Association of Public-Safety Communications Officials (APCO) and the National Association of State Telecommunications Directors, signed a memorandum of understanding with the Telecommunications Industry Association (TIA) in 1992 (amended in 1993) to develop digital LMR standards and public safety requirements. Federal, state, and local public safety representatives worked with the TIA to develop accredited technical standards for LMR systems, known as Project 25 (P25) (Figure 1). As a result of this public-private collaboration, the P25 Suite of Standards has gained worldwide acceptance for public safety, security, public service, and commercial applications. Moreover, P25 standards development is continuous as new features, functions, interfaces, and testing procedures are developed, updated, and released.

P25
DIGITAL WIRELESS • SANS FIL NUMÉRIQUE • INALAMBRICO DIGITAL •

Figure 1: P25 Logo

Adopting Standards

Following the tragic events of 9/11, legislation was passed to improve the interoperability of public safety communications systems and equipment. Congress mandated that new or upgraded equipment must be interoperable and meet certain interoperability standards. As a result, the federal government supported the purchase of P25-compliant LMR equipment through grants and policy to ensure public safety systems can interoperate, regardless of manufacturer.

It is worth noting that while the purchase of P25 equipment provides the technical ability to operate and interoperate, there is an equally pressing need to establish standard operating procedures that define roles, responsibilities, and appropriate usage of dedicated interoperability resources during response operations. Interoperability requires not only the appropriate technology but also the guiding agreements between people, agencies, and other stakeholders to communicate and cooperatively respond to emergencies and disaster events. Recognizing the great value of standards-based equipment investments, the federal government supports the purchase of P25 equipment to improve interoperability among public safety agencies.

Guidance for Purchasing P25 Equipment

The Cybersecurity and Infrastructure Security Agency collaborates with SAFECOM and the National Council of Statewide Interoperability Coordinators (NCSWIC) to provide annual guidance to recipients investing in emergency communications. The *SAFECOM Guidance on Emergency Communications Grants* (*SAFECOM Guidance*) provides recommendations, best practices, and resources for recipients purchasing LMR equipment, including detailed information on P25 standards. Specifically, the *SAFECOM Guidance* recommends that recipients:

- **Read the P25 technical standards for LMR.** The published standards approved by the P25 Steering Committee are available to employees of qualified government agencies at no cost by completing the TIA online request form at: standards.tiaonline.org/all-standards/p25-downloads-application. To date, TIA has published more than 70 standards detailing the specifications, messages, procedures, and tests applicable to the 13 interfaces, multiple feature sets, and functions offered by P25. The test documents include performance, conformance, and interoperability test procedures to ensure baseline compliance with the applicable technical standards. Project and acquisition managers should read any P25 technical standards documents that apply to their system planning or educate themselves before speaking with P25 vendors.
- **Include P25 references in *Requests for Proposals* (RFP) and vendor inquiries.** There are several resources for recipients to reference when developing RFPs and vendor inquiries. These resources help project and acquisition managers to determine which standards are applicable and ensure that proposed projects are compliant with the P25 Suite of Standards. Resources include:
    - P25 Technology Interest Group's (PTIG) *Capabilities Guide*. The guide provides example project requirements and RFPs for agencies to reference. This document and other P25 resources are available on the PTIG website following free registration at: project25.org.
    - *Statement of Project 25 User Needs* (SPUN). Developed by the P25 Steering Committee, the SPUN is a framework for users to better understand P25 technologies and define their communications needs. The SPUN provides high-level explanations of P25 system architecture, features, and functions as defined in the P25 Suite of Standards and recognized by P25 users and system administrators. It translates the more than 70 P25 Standards into relatable content to help public safety officials understand all the capabilities available to them.
- **Select P25 eligible equipment.** To improve interoperability across LMR systems, project and acquisition managers should ensure that digital voice LMR systems and equipment purchased comply with the P25 Standards. The P25 Compliance Assessment Program (CAP) is a formal, independent process created by the Department of Homeland Security (DHS) and operated in collaboration with the National Institute of Standards and Technology. The P25 CAP ensures that communications equipment that is declared by the supplier to be P25-compliant is tested against the standards with publicly available results. As a voluntary program, P25 CAP allows suppliers to publicly attest to their products' compliance with a selected group of requirements through the *Summary Test Report* and *Supplier's Declaration of Compliance* based on the *Detailed Test Report* from the DHS-recognized laboratory that performed the product testing. In turn, P25 CAP makes these documents available, along with a list of grant-eligible equipment, to the public safety community to inform their purchasing decisions at: dhs.gov/science-and-technology/first-responders.
- **Obtain documented evidence of P25 compliance.** Recipients, project managers, and acquisition managers can obtain evidence in one of two ways:
    - Through documented evidence that the equipment has been tested and passed all the applicable, published, and normative P25 compliance assessment test procedures for performance, conformance, and interoperability as defined in the latest P25 CAP's *Compliance Assessment Bulletins* for testing requirements. Before purchasing equipment, managers should confirm whether the vendor has participated in equipment testing consistent with the P25 CAP. If the documentation for applicable equipment is not yet available through the P25 CAP, managers should obtain documented evidence from the manufacturer, as part of the RFP, stating that the applicable tests followed the published test procedures in the P25 Suite of Standards. The manager should also review the published test procedures/standards provided by TIA to identify the appropriate tests and results.

- **Ensure additional features purchased are P25-compliant.** Recipients should ensure that added equipment, features, or capabilities are P25-compliant. Vendor-specific features may not be P25-compliant and, as a result, may hinder interoperability with other equipment and devices that do not share those features. This issue may be especially prevalent in situations where disparate manufacturers' systems will be interoperating. Managers should request the vendor provide a list of non-standard features/functionality and ascertain there is no comparable standard and the use of the feature/function will not impede interoperability with P25-compliant equipment systems. Conversely, managers should also request the vendor(s) provide lists of standardized and non-standardized features, functions, and services confirming that they will yield the expected interoperability in both the same and dissimilar manufacturer deployed systems environments. In addition, when federal grant funds are used to purchase P25 LMR equipment that contains non-standard features or capabilities, where there is a comparable P25 feature or capability available, recipients must ensure the standards-based feature or capability is included as well.
- **If encryption is required, ensure compliance with the P25 standard for the Advanced Encryption Standard (AES), when applicable.** To ensure the interoperability of encrypted communications between public safety agencies, devices used by responders must share a common encryption key and algorithm. The following provides additional guidance on encryption:
  - Recipients using federal funds to purchase encryption options for new or existing communications equipment should ensure that encrypted capabilities are compliant with the current publication of ANSI/TIA-102.AAAD *P25 Block Encryption Protocol* standard.
  - Recipients investing in encryption are strongly encouraged to implement the AES 256-bit Encryption Algorithm as specified in the *P25 Block Encryption Protocol*. The P25 Suite of Standards references AES as the primary encryption algorithm but continues to allow Data Encryption Standard-Output Feedback (DES-OFB) for backward compatibility and interoperability with existing systems. The current version of the *P25 Block Encryption Protocol* should be identified in all procurement actions when encryption is required.
  - Recipients seeking to use federal grant funds to purchase non-standard encryption features or capabilities for new or existing equipment must ensure 256-bit AES is also included to ensure their devices can interoperate in an encrypted mode.
  - Recipients currently using DES-OFB should no longer invest in this encryption method unless the AES (256 bit) encryption is also provided. The continued use of DES-OFB or other non-standard encryption algorithms is strongly discouraged due to security concerns. Recipients should include the anticipated timeline to complete the migration to AES. The federal government recognizes AES as a more robust encryption algorithm and strongly recommends entities migrate to AES as it will enhance interoperability with federal entities, as well as state and local public safety agencies implementing encryption in the future.
- **Provide written justification required for non-P25 purchases.** If a recipient uses federal funds to purchase equipment that is not compliant with P25 Standards, a written justification should be provided to the grantor. Authorizing language for most emergency communications grants strongly encourages investment in standards-based equipment. Many granting agencies will not approve non-standards-based equipment unless there are compelling reasons for using other solutions.
  - Funding requests by public safety agencies to replace or add radio equipment to an existing non-P25 system (e.g., procuring new portable radios for an existing analog system) will be considered if there is a compelling reason why such equipment should be purchased and a written justification of how the equipment will advance interoperability and support eventual migration to interoperable systems. The written justification should also explain how that purchase will serve the applicant's needs better than equipment or systems that meet or exceed such standards. **Absent compelling reasons for using other solutions, public safety agencies should invest in standards-based equipment.**

Conclusion

Standards-based systems enable interoperable communications between responders from various disciplines, jurisdictions, and levels of government in the event they need to communicate during day-to-day incidents, emergencies, and disaster responses. In order to promote interoperability, the federal government strongly encourages public safety agencies to purchase P25-compliant LMR equipment. The *SAFECOM Guidance* and other resources are available to assist recipients in planning emergency communications projects.

About SAFECOM/NCSWIC

SAFECOM includes more than 70 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, emergencies, and natural and man-made disasters. They offer insight 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 the DHS to share best practices and lessons learned with others.

NCSWIC encompasses Statewide Interoperability Coordinators and their staff from the 56 states and territories. The council 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.

Additional Resources

Public safety agencies can reference the following additional materials for more information:

- SAFECOM Technology Resources: This webpage provides guidance and recommendations on communications technologies used in the public safety environment, including multiple LMR and P25 encryption resources such as the *Statement of P25 User Needs*, *Operational Best Practices for Encryption Key Management*, *P25 Inter-RF Subsystem Interface (ISSI) and Console Subsystem Interface (CSSI) Primer*, and *Best Practices for Planning and Implementation of P25 ISSI and CSSI*.
- SAFECOM Guidance on Emergency Communications Grants: This guidance assists state, local, tribal, and territorial entities in applying for federal financial assistance of emergency communications projects. It applies to all federal programs funding emergency communications, providing general information on eligible activities, technical standards, and best practices. For DHS grants, recipients must comply with the *SAFECOM Guidance* as a condition of funding.
- P25 Suite of Standards: TIA's website contains P25 standards development activities that address all technical matters for private radio communications systems and services, including definitions, interoperability, compatibility, and compliance requirements. P25 standards documents are available for purchase. Qualified government entities may obtain copies of P25 standards via the TIA website.
- P25 Technology Interest Group (PTIG): The PTIG website provides information on all P25 Suite of Standards topics. Free registration is required to view content.
- Statement of Project 25 User Needs (SPUN): The SPUN describes user needs and P25 functionality from a P25 users' perspective. This document provides high-level explanations of P25 system architecture, features, and functions as defined in the TIA 102 Suite of Standards and communicated by P25 public safety users and system administrators.
- P25 Compliance Assessment Program (CAP): This program establishes a process for ensuring that equipment complies with P25 standards and can interoperate across manufacturers. P25 CAP helps emergency response officials make informed purchasing decisions by providing manufacturers with a method for testing their equipment for compliance with P25 standards.