Best Practices for Planning and Implementation of P25 Inter-RF Subsystem Interface (ISSI) and Console Subsystem Interface (CSSI): Volume II

July 2020

Federal Partnership for Interoperable Communications
SAFECOM/National Council of Statewide Interoperability Coordinators

Preface

The public safety community continues to emphasize the importance of land mobile radio (LMR) operability and interoperability in the context of industry and budget drivers that are forcing a renewed interest in "doing more with less." As the community seeks to modify existing operational models to ensure sustainability, the interest in Inter-Radio Frequency (RF) Subsystem Interface (ISSI) technology has increased. This document specifically addresses the complexities associated with planning for and executing an ISSI or Console Subsystem Interface (CSSI) implementation. The state and local public safety community, particularly the non-federal members of the Federal Partnership for Interoperable Communications (FPIC) ISSI/CSSI Focus Group,[1] noted the need to share ISSI/CSSI best practices within the community to aid others in the planning and implementation processes.

It is essential that public safety agencies comprehensively understand all aspects of planning and implementation, including partnerships and governance,[2] identifying and engaging stakeholders, assessing technology, crafting and updating policies, and establishing operations and maintenance (O&M) requirements that may arise in a shared resources environment. **Volume I** focuses on suggested pre-planning, partnerships, and governance elements; it provides best practices observed during the initial planning stages by local, county, regional, and state agencies implementing ISSI and/or CSSI and should be reviewed prior to, or in parallel with, Volume II. This volume (**Volume II**) covers other planning and implementation components (e.g., stakeholders, technology, policies, O&M), as well as addresses various implementation best practices for agencies contemplating or proceeding with installation of an ISSI and/or CSSI solution.

This document is a result of extensive collaboration of the FPIC ISSI/CSSI Focus Group whose membership is outlined in **Appendix A: Contributing Agencies**.

---

1 The FPIC is recognized as a technical advisory group to SAFECOM and the Emergency Communications Preparedness Center.

2 In the SAFECOM Program's Interoperability Continuum, governance is one of the five identified critical success elements that must be addressed to achieve a sophisticated interoperability solution. The Interoperability Continuum is designed to assist public safety agencies and policy makers plan and implement interoperability solutions for data and voice communications.

Executive Summary

Project 25's (P25) accredited technical standards define features, functions, and the interfaces of P25-compliant radio systems. Two of these interfaces, the ISSI and CSSI, are designed to enhance the operability and interoperability of new and existing land mobile radio systems. ISSI technology permits multiple radio core systems or Radio Frequency (RF) subsystems to be connected and form larger wide-area networks, supporting the "system-of-systems" concept. The CSSI interface can provide interoperability among multiple dispatch console manufacturers' and system infrastructure manufacturers' console product offerings, which enables public safety agencies to implement third party P25 console systems.

Given increased interest in both ISSI and CSSI technology, the Federal Partnership for Interoperable Communications, supported by the **Cybersecurity and Infrastructure Security Agency** (CISA), established the ISSI/CSSI Working Group (comprised of users and manufacturers) and the Focus Group (users only) to explore the ISSI/CSSI technology environment. Among other topics, the Working Group and Focus Group continue to explore connecting single and multiple manufacturers' ISSI or CSSI technology offerings; collect user and manufacturer implementation procedures and troubleshooting methods; and identify best practices and commonly identified implementation and operational challenges in an ISSI and/or CSSI environment.

This document outlines categories for practitioners to consider when planning for and implementing ISSI or CSSI technologies. The high-level categories are rooted in best practices observed during all project phases by local, county, regional, and state agencies implementing ISSI/CSSI and are provided as a resource for others in the community who may be contemplating or proceeding with ISSI/CSSI implementation. The six categories are listed in **Figure 1** in the corresponding volume.

Figure 1: ISSI and CSSI Best Practices Volumes and Topics

VOLUME I
• **Pre-Planning –** This category can include a nearly endless set of questions and topics to consider before planning and implementing an ISSI or CSSI, including articulating the underlying purpose, identifying potential partners, setting expectations, conducting a cost-benefit analysis, and pursuing education or training to sufficiently understand the technologies. • **Partnerships and Governance –** Governance is one of the critical success elements that must be addressed to achieve and maintain a sophisticated interoperability solution. This category includes establishing trusted relationships, expressing a desire to interoperate, solidifying partnerships, and establishing formal governance structures via documentation that addresses everything from roles and responsibilities to financial and budget considerations.
VOLUME II
• **Stakeholders –** It is critical to identify the "right" stakeholders to be involved in planning and implementation, including key leadership, radio systems provider personnel, network professionals, manufacturer personnel, consultants, technical experts, and end users. • **Technology –** The selection and implementation of offered technology solutions and associated features and functions presents many potential challenges that user agencies must understand and be prepared to address. • **Policies –** Partnering agencies must establish standard operating procedures and policies to address everything from talkgroup management to fleet mapping and from user protocols to software and hardware version controls. • **Thinking Ahead –** Throughout planning and implementation, agencies must constantly look ahead and plan for various elements, including continuing active coordination of operations and maintenance, future upgrades, and new or revised feature implementations.

Table of Contents

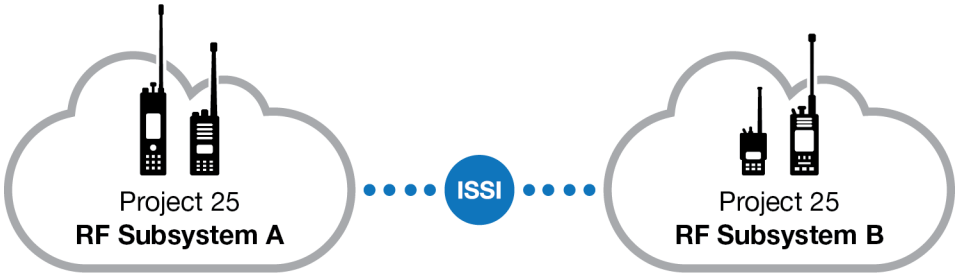
List of Figures

Background

P25 is an open-architecture, user-driven suite of digital radio communications accredited technical standards developed and used by federal, state, tribal, territorial, and local public safety agencies to enable LMR radio interoperability. As public safety radio systems transitioned from analog to digital technologies in the 1980s and the implementation of trunked radio systems increased significantly, agencies sometimes found it difficult to operate, interoperate, and effectively communicate information across jurisdictions and agencies due to differing systems with varying digital protocols implemented by different manufacturers. P25's open standards define the interfaces, as well as the features and functions of P25-compliant radio systems.

As one of eleven currently defined component interfaces codified during P25's continuing standards development, the ISSI provides a standardized, non-proprietary Internet Protocol (IP) connection of two or more P25-compliant systems. These ISSI enabled radio system cores or RF subsystems (RFSS) may be from different manufacturers, may operate in different frequency bands (e.g., very high frequency [VHF], ultra-high frequency [UHF], 700/800 megahertz [MHz]); using different versions of P25 (Phase 1 or Phase 2), or all the above. The basic requirement is that each radio system core or RFSS must incorporate an ISSI interface. In other words, ISSI technology allows for multiple radio system cores or RFSSs to link together and form larger wide-area networks, supporting the "system-of-systems" concept.

Figure 2: ISSI Example



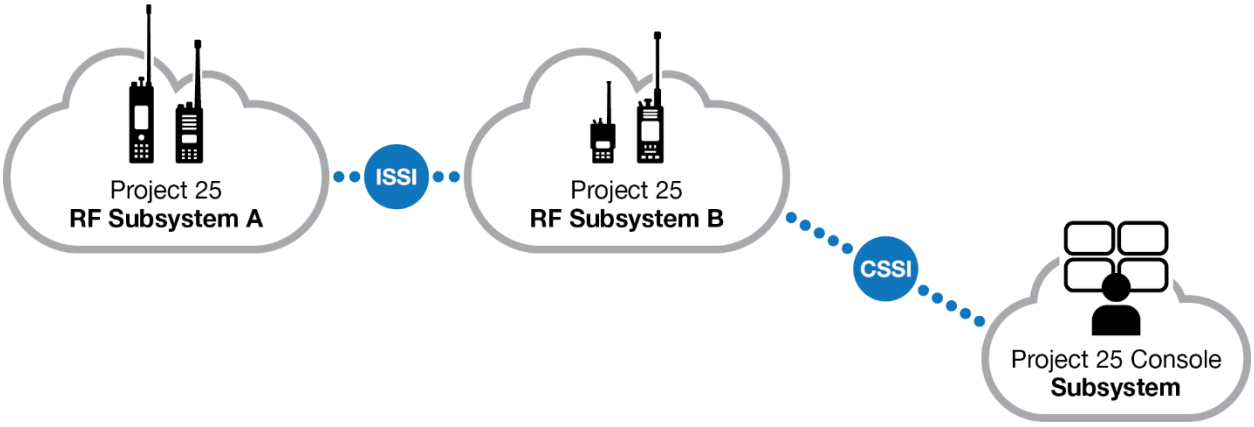
A system-of-systems approach relies on an agency's ability to own and manage an independent system while collaborating and sharing resources with other local, regional, state, tribal, and federal systems. Using a system-of-systems approach, each individual system or RFSS becomes a component in an extended communications network, which could be potentially countywide, multi-county, regional, statewide, or even a nationwide grouping of connected systems. Each system can be connected to others if jurisdictions and agencies effectively collaborate through establishing governance structures, identify compatible technology and equipment, creating standard operating procedures (SOP), and design and implement training exercises and drills for use today and in the future. These technical connections and trusted relationships among jurisdictions and agencies establish the foundation of a system-of-systems construct and lay the groundwork for successful interoperability and enhanced operability.

When paired with appropriate systems planning and management, SOPs, and recurring training, ISSI can be a valuable tool to increase the efficiency and reliability of interoperable communications during both emergency response and normal day-to-day activities. A properly configured ISSI can provide substantial extensions to a system's coverage area using the connected systems resources and can more effectively facilitate automatic and mutual aid scenarios among jurisdictions.

CSSI is another wireline interface included in the P25 standards, which permits a standardized IP connection between the RFSS and console equipment. Prior to the development of the Digital Fixed Station Interface (DFSI) standard for P25 conventional systems, public safety communications centers had few choices for console system solutions. Each infrastructure manufacturer had its own proprietary solution for connecting console equipment to the RFSS. As P25 moved toward digital IP connectivity, console systems typically had linked to the RFSS via analog signaling. The development and issuance of the CSSI interface standard brought the same level of standardized IP connectivity to the P25 trunked RFSS environment. The CSSI provides for interoperability between multiple dispatch console manufacturers' offerings and system infrastructure manufacturers, which enables third party P25 console options. The use of CSSI allows implementing agencies to have additional console equipment choices during acquisitions, which may better address identified operational requirements.

Planning must include identification, analysis, and understanding of all potential capital and recurring costs, including costs to plan, implement, and maintain the ISSI or CSSI solution and train personnel, as well as soft costs incurred while pursuing a complex engineered solution.

Figure 3: CSSI Example



Planning and Implementation Best Practices

In January 2019, the FPIC[3] ISSI/CSSI Focus Group published *Best Practices for Planning and Implementation of P25 Inter-RF Subsystem Interface (ISSI) and Console Subsystem Interface (CSSI): Volume I* in association with **SAFECOM** and the **National Council of Statewide Interoperability Coordinators (NCSWIC)**. In this document, the Focus Group identifies six critical categories of ISSI/CSSI planning and implementation (see **Figure 4**). Pre-planning is followed by a combination of establishing partnerships and governance, identifying the "right" stakeholders to be involved in planning and

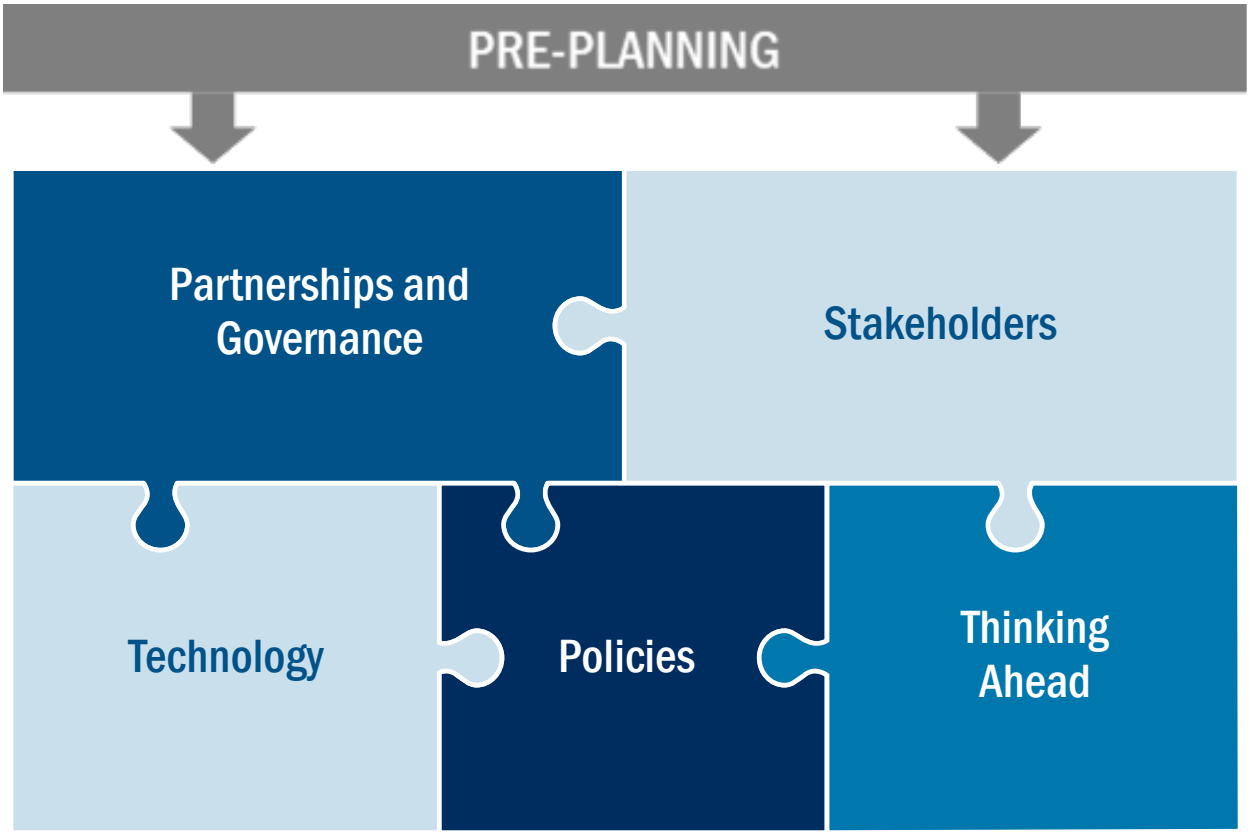
[3] The FPIC serves as a coordination and advisory body to address technical and operational wireless issues relative to interoperability within the public safety emergency communications community. The FPIC serves as an interface between the federal, state, tribal, and local agencies. It includes more than 200 federal, state, local, and tribal public safety representatives from over 45 federal agencies, as well as representatives from state, tribal, and local entities.

implementation, assessing and implementing technology solutions, creating policies (e.g., SOPs), and thinking ahead to plan for maintenance and upgrades.

Volume I specifically addresses pre planning and partnerships and governance; this document also introduces the inherent complexities associated with pursuing an ISSI or CSSI implementation. The Focus Group's experience is such that each implementation is different, which further emphasizes the importance of all planning elements. Per Volume I, pre-planning can include a nearly endless set of questions and topics to explore as an agency considers the viability and feasibility of implementing an ISSI or CSSI solution within its current communications landscape. For example, it is important to understand the purpose, underlying motivations, and desired outcomes of pursuing ISSI connections to and from other stakeholders. Additionally, pre-planning should include analyzing and cataloging all potential costs associated with an ISSI or CSSI implementation; a cost-benefit analysis must be understood by all potential participating agencies and their governing authorities. Governance refers to establishing a shared vision coupled with an effective organizational structure to support any project or initiative that seeks to solve interoperability issues.

The ISSI/CSSI Focus Group has continued to discuss, identify, and document challenges associated with ISSI and CSSI implementations and thus developed this second volume to specifically address stakeholders, policies, technology, and thinking ahead.

Figure 4: ISSI/CSSI Planning Components



STAKEHOLDERS

People are as important as the technology itself, and it is critical for all agencies to identify the "right" stakeholders to be involved in planning and implementation. Given the technical complexities

of an ISSI or CSSI implementation, it may be tempting to leave radio and console end users (e.g., emergency management, emergency medical services, fire, law enforcement, and emergency communications centers), as well as radio and network personnel to their own devices. However, a diverse team of agency and partner agency leadership, communications systems provider personnel, and IP network professionals, as well as manufacturer personnel, consultants, technical experts, procurement professionals, and radio and console end users from all affected agencies or disciplines will yield the best overall results. Additionally, the "right" stakeholders should have the participating agencies' best interests in mind with respect to interoperability. This part of planning can happen after partnerships and governance are established or in parallel.

One Size Does Not Fit All

The depth and breadth of individuals from each agency involved in ISSI or CSSI discussions varies significantly from implementation to implementation; however, these individuals generally possess a distinct combination of enthusiasm and technical acumen to drive the solution forward. For some proposed projects, practitioner-level discussions incorporating radio systems management personnel generates sufficient interest and enthusiasm and allows for timely and efficient implementation. For others, an ad hoc group or formal subcommittee or working group(s) within the established governance structure may be the appropriate venue to engage stakeholders for successful coordination. Still others may require engaging the full gamut of agency personnel from system managers to networking stakeholders to cyber and information technology (IT) security personnel. If the project gains traction and becomes "real" and depending upon scope, most if not all of these specialties will likely become, or should become, involved and tasked for a successful implementation.

Some agencies may need to specifically engage non-technical personnel or individual champions to help secure funding from budgetary entities (e.g., state legislatures, city councils, county commissions, joint powers authorities) or promote educational campaigns to obtain community or leadership buy-in. These champions must help the agencies interested in establishing ISSI connections sell the concept and associated benefits to everyone from city councils to mayors to public safety agency leaders. Depending on the audience, these champions could be everyday system users – the public safety stakeholders themselves. Though they may be unfamiliar with the specific technical solutions such as ISSI, public safety stakeholders can genuinely articulate the specific requirements – "the why" – for interoperability in day-to-day operations, as well as incident response. They can also leverage real-world examples of communications failures or identified but unfulfilled needs in their communities to demonstrate the pressing need for improved operability and interoperability.

Other situations may call for agency leaders, partner agency leaders, or simply interested or knowledgeable advocates (e.g., state agency personnel, federal partners, representatives from other successful ISSI implementations) to speak on behalf of the proposed project to illustrate potential successes, acknowledge possible challenges, and introduce mitigation strategies.

Radio Personnel

The most obvious stakeholder group to include in an ISSI or CSSI implementation is radio systems management personnel, including agency radio system administrators. In many cases, these individuals are driving implementation themselves and are a catalyst for change within their respective organizations. They bring critical skills, institutional knowledge, and experience, including working knowledge of the agency's existing P25 system. However, given the complexities and nuances inherent in the P25 standards, it is important for an agency to recognize and address any knowledge limitations (i.e., "what you know," "what you don't know," and "what you don't know you don't know"). The Focus Group suggested that agencies establish a baseline understanding of what

the P25 standards call for, which features the standards enable, and which decisions are left to the manufacturers and users directing the implementation. Additionally, as stated in Volume I, the Focus Group noted a best practice is to attend prospective manufacturers' in-depth technical courses to develop a thorough understanding of what ISSI/CSSI enabled systems can and cannot do and specifically what features and functionalities the manufacturers can and cannot offer via the ISSI or CSSI technology. If the P25 systems are already in place, radio personnel should attend training offered by the host system manufacturer, as well as the connected system manufacturer (if different).

It is important to note that planning for a potential ISSI or CSSI solution must take place in the context of the existing (or proposed) P25 system(s); the solution will not exist in a silo and must be considerate of the larger communications environment.

Network Professionals

The Focus Group strongly suggests that agencies engage the network professionals, engineers, or architects responsible for the IP-based network that serves as the backhaul connectivity for the ISSI implementation. These personnel may not have previously engaged with radio systems technologies and may require education and perspective on the project at hand. It is important to set expectations with network personnel around necessary support, the (potentially extensive) time commitment required, and the complexities of working with various manufacturers to implement a ISSI or CSSI solution.

Agencies should conduct an inventory of available technical resources (e.g., knowledge, skills, abilities) to determine if they need to budget to hire adjunct personnel with a specific skill set or request that manufacturer(s) provide certain knowledge/skills.

Network planning requires the identification and inclusion of a complement of skilled networking/internetworking personnel to identify, develop, and potentially provide connectivity resources, IT/IP network analysis or troubleshooting tools, and maintenance of required networking components to effectively support the ISSI/CSSI connectivity. These individuals can also provide critical knowledge and support regarding relevant security protocols. Network-related stakeholders may include entities beyond those that have direct relationship to the ISSI/CSSI or wireless communications systems. These personnel can work directly with the ISSI manufacturer on the necessary network configurations, incorporate the ISSI networking requirements into an existing enterprise network topology, assess and configure routers, and update firewall management, as needed. They can also provide critical redundancy, resiliency, and back-up for this "always on, always available" connectivity and first-hand knowledge when manufacturers suggest that issues stem from the network itself. The right team can contribute directly to problem-solving, save time and money, and minimize frustration for the implementing agency(ies).

The Focus Group acknowledged that not all agencies have a dedicated institutional network team. Agencies may need to depend upon IT departments to facilitate or hire external expertise or pay the manufacturer for the services to make the necessary network connections, align configurations, and setup processes to ensure consistent operations.

Radio and Console End Users

Another key stakeholder group to include in planning and implementation efforts is end users from all affected agencies or disciplines. This group may include command staffs, police officers, firefighters, emergency medical services personnel, public services or public works entities, transportation agencies, 9-1-1 telecommunicators, and dispatchers – effectively anyone who is going to end up using the implemented solution. The implementing team may want to identify a complement of engaged users from each subgroup to define tactical goals, objectives, and operational scenarios that can then be used to drive comprehensive requirements development and then assess manufacturer proposals.

Simultaneously, this provides an opportunity for expectation setting with involved users to explain what the proposed ISSI or CSSI can and cannot do and how it will function in day-to-day operations. For example, the Focus Group noted the importance of specifically asserting the expectations of features and functions cannot be understated. While everybody wants the ISSI connection to allow all the features and functionality that exist on a home system to be present on the connected foreign system, the desire is not likely to be met, especially when disparate systems connection is under development. This information is critical for the development of user requirements and SOPs, protocols, and other user guidance.

Manufacturer Personnel

Given experiences to date, the Focus Group strongly suggests agencies engage potential manufacturers before acquisitions and employ comprehensive fact-finding discussions to fully understand the proffered solution(s) and associated features. By actively engaging with manufacturer personnel, agencies can develop a sense of manufacturer-specific jargon and nomenclature to then understand how the product(s) relates to other offerors and their ability to successfully interoperate or not.

It is important to engage the "right" manufacturer personnel at all stages of planning and implementation. Though there is a role for project managers and sales staff, agencies should oblige manufacturers to facilitate agency engagement with seasoned project integration engineers and product design engineers who have explicit and recent experience implementing a similar ISSI or CSSI project. The Focus Group suggested including specific manufacturer personnel requirements (e.g., common titles, qualifications) in procurement and contractual documents to ensure the necessary support. Experienced manufacturer implementation teams can mitigate the burden placed on agency personnel and facilitate a timelier execution and completion of the project at hand. If the local radio shop is appointed responsibility for the implementation, agencies should work directly with those personnel but strongly encourage them to reach back to the manufacturer for support, advice, and guidance. Even the most skilled local vendors may not have the specialized skill sets required for successful implementation.

Agencies should leverage organizations (such as FPIC) or solicit guidance directly from other jurisdictions that worked with the same manufacturer(s) to identify and target knowledgeable manufacturer personnel to assist in project execution, as needed.

TECHNOLOGY

The technology component of any ISSI or CSSI implementation is inherently complicated. Though the technology is standards-based and often marketed as "plug and play," the Focus Group participants have experienced first-hand the challenges that required meticulous planning and dogged commitment to manufacturer coordination to ensure a successful technology implementation. Their collective experiences demonstrate ISSI/CSSI technologies are not "plug and play" add-ons to P25

communications systems. These technologies are engineered solutions that require detailed analysis and comprehensive technical planning. As technical requirements expand to accommodate additional features and functions between connected systems, implementation becomes increasingly complex. Agencies must evaluate numerous facets, components, and configuration options of the overall P25 system to ensure that the ISSI/CSSI will provide the expected results; this complexity is further exacerbated when connecting disparate systems from different manufacturers.

This section cannot begin to cover all aspects of technology planning and implementation, and it will not address implementation challenges (see the **Project 25 Inter-RF Subsystem Interface (ISSI) and Console Subsystem Interface (CSSI) Primer** ["ISSI and CSSI Primer"] for primary planning and implementation challenges). Rather, the focus is on general best practices, as well as best practices associated with five key technology areas (i.e., network connections, infrastructure, consoles, subscriber units, and features).

General

The Focus Group noted several general technology-related best practices. First, the group suggested conducting a full inventory of all current technology, including but not limited to, network paths, radio systems infrastructure, consoles, voice recorders, subscriber units, and software, hardware, and firmware versions and revision numbers. This effort allows agencies to ensure that the existing systems and their associated components are ISSI or CSSI ready. See **Figure 5** for a series of relevant questions to consider.

Figure 5: Items to Consider as a part of a comprehensive technology inventory.

SAMPLE QUESTIONS
• Will the existing subscriber units (hardware and software versions) and infrastructure support the expected ISSI version? • Does the existing peripheral equipment (e.g., consoles, logging recorders, connectivity) have excess capacity or the ability for expansion to support the ISSI talkgroups and concurrent connections expected between cores and/or RFSSs? • Will the existing enterprise, private, or commercially available network connectivity effectively support the required connections between ISSI/CSSI components positioned at participating agencies (e.g., available bandwidth, connection health, latency, uptime availability)? • Is redundant connectivity with automatic switchover available between ISSI connections? • Is active monitoring of connectivity available for critical connections? • Evaluate existing coverage/capacity of potential foreign sites that may be available for coverage expansions via the ISSI. • Evaluate participating agencies' current processes and methods of subscriber unit identification and consider a unique numbering plan for all participating agencies to ensure uniqueness. • Evaluate participating agencies' current processes and methods of subscriber unit alias use. Consider unique aliases or incorporating agency IDs within assigned aliases for all participating agencies to ensure uniqueness (anticipation of alias transmission over ISSI). • Evaluate how encryption services will be administered in an ISSI connected environment and how methods and procedures may change and require updates. • If relevant, have components undergone cybersecurity audits?

Conducting an inventory and answering these questions should help agencies calculate the potential capital outlay required to either acquire replacement or new equipment, as well as estimated recurring O&M costs for network interconnection(s), software licensing, equipment, programming, and other services.

Second, the Focus Group emphasized the importance of comprehensive standards compliance and interoperability testing, validation, and acceptance. Given that standardized ISSI/CSSI interoperability testing remains undefined, the Focus Group suggested that compliance checking, both P25 Compliance Assessment Program (CAP)- and procurement-driven, along with adequate interoperability testing must be featured and agreed upon by the purchasing agencies and the supplying manufacturers. The Focus Group suggested agencies engage with a body, such as FPIC, or directly with other jurisdictions that have similar ISSI or CSSI configurations to understand the test plans and procedures used and any specific challenges.

Network Connections

To establish an ISSI connection, the participating agencies must first establish a secure network backhaul or connectivity between the connecting systems. In some situations, agencies may be able to leverage an existing agency-owned fiber and/or microwave connection for the ISSI link; in others, agencies may be forced to interconnect fiber from different commercial carriers to complete the pathway between systems or to use a combination of both. The network services requirements likely include robustness, redundancy, and resiliency of the envisioned connections between the core(s) or RFSSs. For operational parameters, agencies need redundancy; for mutual aid, the original setup could leverage a single link with a plan to add duality at a later date. One agency noted that given the operational nature of its ISSI and previous network connection failures, it requires a primary and secondary connection and now uses twin T-1 connections. Agencies must contemplate the ability for existing sites or current connectivity to support additional capacity or additional physical connections and related equipment into existing facilities.

The Focus Group noted that when using commercial services, agencies should work closely with the commercial carriers and the relevant manufacturer(s) to ensure the proper configuration of firewalls, port accessibility, routers, switches, servers, virtual private networks, rules, and latency timing, as well as clarify cybersecurity roles and responsibilities. This attention to detail is required to appropriately address nuances in specific manufacturer ISSI/CSSI configurations and ensure that these settings and network configurations may be maintained to support a persistent, uninterrupted connection; additionally, special care must be taken when multiprotocol label switching (MPLS) networks are involved. Agencies should be aware of regulatory and/or state laws that may potentially require agencies to directly engage with common commercial carriers and prevent contract options from superseding such engagements. As such, one New York agency included language in its contracts with its successful manufacturer that requires said manufacturer to provide its exact backhaul circuit requirements, so the agency could then equitably and thoroughly assess commercial carrier proposals to provide the required connectivity.

No matter the network provider, the Focus Group recommended a series of questions to confirm network accessibility and availability:

- Is there network connectivity at the desired locations? If not, can it be obtained? What is required to extend network connectivity to the relevant locations? What are the implications for overall implementation schedule?
- What capital and/or O&M costs are associated with the network connectivity?
- Does the network have sufficient capacity to handle the additional data loads from ISSI traffic now and into the future as additional applications and requirements are added to subscriber units?
- What, if any, additional effort is required to address relevant cybersecurity requirements?
- Is active monitoring of connectivity available for critical connections?

Infrastructure

Agencies must consider the existing, underlying P25 systems in the planning process. As previously stated, the ISSI or CSSI solution will not exist in a silo and must be considerate of the larger regional communications environment. The Focus Group identified several best practices relevant to different aspects of the underlying infrastructure. For example, agencies should identify current and expected loading requirements and any system constraints, or in other words, develop a thorough understanding of each underlying system's talkgroup and user capacity and ensure that enough capacity exists in all connected systems for normal day-to-day activities, as well as extraordinary occurrences once the ISSI is implemented.

From a hardware perspective, agencies should identify opportunities to collocate equipment at existing infrastructure sites with partnering agencies. Several Focus Group participants noted collocating equipment or similar bartering was simpler to execute than transferring funds among partnering agencies. As stated above, a comprehensive inventory allows an agency to identify hardware that may need to be replaced in advance of an ISSI or CSSI implementation.

Furthermore, if the proposed ISSI or CSSI connections are between or among disparate manufacturer systems, agencies should take the time to understand site and core equipment, peripheral equipment, software revision, and ISSI/CSSI software/hardware licenses required to enable interoperable communications across the connection(s).

Consoles

Consoles play a key role in both ISSI and CSSI implementations. An agency implementing an ISSI solution should evaluate console subsystems to ascertain their ability to actively support potentially large numbers of additional ISSI talkgroup resource appearances on consoles, as well as the ability to effectively manage and manipulate those resources via the consoles.

The use of CSSI allows agencies participating in a wide area system of systems environment to select a console solution that offers the best set of console features and functionality to meet the agencies' specific needs, as well as operational budget. An agency should clearly define and document needs and requirements, including the desired operational characteristics and ergonomics of the features and functionalities. Additionally, the Focus Group noted that the introduction of non-native consoles to an existing P25 system will likely incur licensing fees that should be appropriately accounted for when calculating the total cost of implementation, including both capital and operating expenditures. Finally, though multiples CSSIs can be supported with a wide area system of systems environments, doing so increases the complexity of overall systems management and implementation.

Subscriber Units

An agency should clearly articulate its approach to subscriber units on its system, especially in the context of an ISSI or CSSI implementation. It must decide if it wants to allow multiple manufacturer offerings, and then inside those offerings, identify the required and optional features. Or, alternatively, an agency can simply identify a single approved subscriber unit for the network. One east coast agency noted it allows a single subscriber unit that allows for over-the-air rekeying and over-the-air programming. In contrast, a western state allows subscriber units from three manufacturers on its statewide system and has a process in place to test models against an existing template; the state does not guarantee that additional options and features will work on the system. Another agency in the northeast indicated it is evaluating multiple subscriber units and will create a list from which any future partner agency can choose; only the listed subscriber units will be allowed on the system, which will ensure a consistent user experience for public safety.

Several midwestern states leverage an operational test document to understand how subscriber units will perform on a given deployment or system configuration. The Focus Group noted that even though units undergo P25 CAP testing, it is important to understand how subscriber units will behave on your network. This applies to both new subscriber units and updated firmware in existing units. Not all subscriber units will operate within or appropriately support the ISSI-connected environment. Thus, the aforementioned call for a comprehensive inventory (see "General" section above) will allow the model numbers and software version(s) to be included in procurement documents to ascertain if none, some, or all subscriber units will need to be replaced or updated to allow proper functionality with the ISSI and stated requirements.

Additionally, when working through a CSSI implementation, agencies should not lose sight of the role that subscriber units can and will play. One agency shared it did not include subscriber units in its overall implementation planning, which resulted in several issues that ultimately required software updates to all subscriber units.

The Focus Group also noted that agencies should consider other elements related to subscriber units, including user licenses and dimensioning of subscriber databases.

Features

As stated in the **ISSI and CSSI Primer**, "[m]anufacturers are not required to implement a feature that is defined in an accredited technical standard, and there are instances in which the standard does not specify how a feature is implemented;" thus, the method of implementation is at the manufacturer's discretion. This can result in discrepancies between manufacturers in how they implement the ISSI/CSSI standards and how the actual features and functions, facilitated through an ISSI or CSSI, may or may not operate or interoperate as expected. These discrepancies can introduce implementation issues, especially when attempting a connection between disparate manufacturers' systems." To mitigate these kinds of issues, several east coast agencies implementing an ISSI compelled their respective manufacturers to collaborate; identify and test mutually supported, interoperable features; and flag any operational constraints. This exercise to cross-walk features is a best practice that agencies should consider. Though potentially time consuming, the knowledge gained by all parties is invaluable.

The Focus Group noted other best practices associated with features. For example, encryption is a technical element that must be embedded in pre-planning. Encryption gets particularly complicated when implemented over an ISSI connection, especially a connection between disparate manufacturers. One agency noted that it opted to carry a single encryption key to simplify operations for the end users; this same key also serves as the patch key to minimize challenges when patching talkgroups.

Though this document is focused on best practices rather than implementation challenges (see ISSI and CSSI Primer for sample list of implementation challenges), the Focus Group felt obligated to address several ISSI/CSSI features that continue to challenge group members on a regular basis. The ISSI/CSSI features in question include the ability to supergroup or group talkgroups, as well as the activation and clearing of emergency alarm or emergency alerts on consoles in ISSI environments of different manufacturers' systems. The implementation or operational challenges presented by these features stem from, as previously expressed, discrepancies among manufacturers in how they implement the ISSI/CSSI standards. The Focus Group suggested a best practice is to understand these challenges going into an ISSI/CSSI implementation and consider them when making procurement decisions.

For example, one agency noted that if a console does not allow for patch creation on a disparate manufacturer's system, then the only option is to acquire consoles from the system manufacturer;

this inherently eliminates the flexibility intended by the CSSI standard. Related to clearing emergency alarms or alerts on consoles, the Focus Group noted the best practice is to understand the limitations and plan ahead; work with implementing partners to draft SOPs for emergency communications center staff to clear alarms and alerts both systemwide and locally.

It should be noted that the P25 CAP is currently exploring testing for a few ISSI/CSSI features and functions. In the interim, manufacturers have been doing lab-to-lab testing of commonly supported ISSI/CSSI standard feature sets. The P25 Technology Interest Group offers a testing template[4] that describes a method for reporting ISSI and/or CSSI P25 interoperability testing results outside P25 CAP. The template does not intend to prescribe a list of standard functionality that could or should be tested. The functionality covered by a published report should be determined by the manufacturers completing the report.

POLICIES

Another aspect of planning and implementation of ISSI and CSSI solutions is the crafting of relevant policies and procedures. As noted in Volume I, governance "[a]greements should include a commitment to craft shared operational policies for the use of the system(s) and the expected interactions among participating agencies."[5] The Focus Group identified a series of example policies and procedures that would be relevant to ISSI and/or CSSI implementations. The list in **Figure 6** is by no means inclusive of all potential policies, but it serves as a starting point for agencies to consider.

Figure 6: Example policies and procedures to agency consideration and development.

POLICIES AND PROCEDURES
• Establish SOPs for provisioning user equipment IDs (e.g., unique ID planning, statewide ID plans), talkgroups, and group affiliation, as well as adding new users • Establish shared SOPs for ISSI talkgroup use, including the number of talkgroups allowed, specific uses for specific talkgroups, number of users allowed, and who can be on what group based on loading and system constraints • Define specific procedures for managing the ISSI connectivity and procedures for connection interruptions, including who to notify and in what order • Create a regional shared talkgroup memorandum of understanding or policy to allow radio users access to partnering systems • Establish software/hardware version control of ISSI, CSSI, and subscriber units, including testing requirements before scheduling and implementing any software updates • Establish procedures for encryption and key management

The Focus Group noted that policies may also include additional governance structures, as needed. For example, if an agency is leveraging an existing or new regional IP network, a best practice would be to establish or amend existing regional IT governance for the overall network responsibility, including network lifecycle and expansion. The IT governance structure should address network

[4] Project 25 Technology Interest Group. "ISSI/CSSI Non-CAP Interoperability Testing Template." Version 2, updated January 17, 2019. Available online: http://www.project25.org/index.php/compliance-assessment/p25-non-cap-issi-cssi-interoperability-testing.

[5] In the SAFECOM Program's Interoperability Continuum, governance is one of the five identified critical success elements that must be addressed to achieve a sophisticated interoperability solution. The Interoperability Continuum is designed to assist public safety agencies and policy makers plan and implement interoperability solutions for data and voice communications.

monitoring, identify maintenance windows, define outage notifications and reporting criteria, and explain how to onboard new agencies/services to the network.

Additionally, agencies should define policies and procedures for initial and periodic training of all involved personnel from users to system administrators. Standardized basic training prior to activation should include all new features, functions, and capabilities and relate back to the operational scenarios used during requirements definition and expectation setting. As new or updated features are introduced, additional training with commensurate SOPs should be provided. Over time, recurring operational training benefits all personnel, but agencies must be sure to update said training or refreshers to reflect new or updated ISSI/CSSI functionality. Agencies should also identify opportunities to use or incorporate ISSI features and functionality into planned exercises to ensure user proficiency.

THINKING AHEAD

Throughout the planning and implementation process, agencies must be "thinking ahead" and preparing for the on-going operations and maintenance of the ISSI or CSSI solution. The Focus Group specifically noted that agencies should compile budgetary estimates of the recurring O&M costs for network interconnection(s), software, hardware, connection/seat/device licensing, equipment, and services and add those costs to proposed out year O&M budgets. These budgets should also consider any components that will lose warranty coverage during the budget cycle. Furthermore, as ISSI/CSSI implementations are complex, engineered solutions, participating agencies should consider adding a contingency element to capital and O&M budgets that can defray unforeseen costs that may arise and significantly impact the success of the implementation. O&M costs must also be discussed among participating agencies to determine the appropriate cost sharing going forward. Additionally, agencies should consider plans for maintenance, upgrades, and on-going testing/reporting.

Maintenance

Figure 7: Key elements of a maintenance plan or agreement.

POLICIES AND PROCEDURES	
A thorough maintenance plan should:	
• Require timely notifications of outages and define the timeline for notifications • Define timelines for maintenance responsiveness (e.g., within two hours) • Outline specific maintenance windows	• Describe maintenance communications process for sharing information among participating agencies • *Optional:* Allow for purchase of additional equipment or software, as needed

Agencies should develop a maintenance plan that defines the overall maintenance processes, including roles and responsibilities of participating agencies. This should include identifying specific maintenance stakeholders that will provide continuing maintenance and upkeep of equipment, services, and resources to meet operational scenarios and requirements. These individuals may be among those individuals previously identified in the Stakeholders section (e.g., radio personnel, network professionals), but it is important to address the on-going role that these personnel will play going forward. Alternatively, the maintenance plan may identify specific services that will be outsourced to commercial vendors for the continuing maintenance and upkeep.

One organization operating under a joint powers authority agreement explained two participating counties have contracts to provide maintenance and technical support from the respective radio shops on a 24/7 basis or as needed, depending on the contract. This organization also has a

contract with the primary manufacturer that covers upgrades for all computers, switches, and routers every year. The service plan includes specific response times, as well as specifies the availability of the original program manager and technicians.

Updates

The Focus Group noted that system upgrades can be particularly complicated with an ISSI or CSSI solution as they may impact subscriber units, consoles, and infrastructure equipment. Agencies, in collaboration with system manufacturers, should develop a comprehensive plan that identifies the process for system upgrades and software/hardware revisions over the anticipated life of the system. Specific things to consider include:

- **Contracts:** Ensure manufacturer contracts explicitly state the amount of time the contracting public safety agency receives free upgrades and a graduated lists of costs and/or cost increases of the out years after warranty on agreement expirations.
- **Partner Coordination:** Coordinate with partner agencies regarding all system upgrades. Review release notes to identify any changes that might cause problems with the existing systems configurations and equipment. Again, leverage organizations, such as FPIC, to identify jurisdictions with similar configurations to obtain insight regarding any known issues with a given upgrade.
- **Pre-Upgrade:** Identify if any of the partnering agencies have available non-production capacity, environments, or labs to test and evaluate changes and upgrades before they are released and implemented in the production environment.
- **Post-Upgrade:** Execute the test procedures that were used during initial implementation to quickly identify any potential issues. Revisit prior successful conformance and interoperability testing to ensure new changes are stable, pass testing, and provide the new feature/function with the expected results.

Conclusion

ISSI and CSSI connections can greatly enhance emergency communications interoperability between different radio systems of the same or disparate manufacturers. These connections allow public safety agencies to extend their LMR networks, roam into neighboring communications systems while maintaining connectivity to their home systems, as well as communicate with responders from different jurisdictions and agencies. These connections have facilitated critical mutual aid communications during planned events and emergencies. ISSI and CSSI also provide organizations with the flexibility to purchase communications equipment from multiple vendors and maintain independent systems while connecting to other agency networks, if necessary. Agencies looking to expand LMR coverage and enhance interoperability among partner agencies and jurisdictions should further research ISSI and/or CSSI to determine if these connections would be a viable solution.

Implementing an ISSI or CSSI will likely present a series of challenges for the implementing agencies and requires careful planning from including the “right” stakeholders to inventorying technology to prescribing policies and preparing for future upgrades. While challenges can be formidable, the resulting enhancements to overall system operability and interoperability can be significant. If agencies leverage the best practices articulated in this document, those agencies will be better positioned to mitigate or at least address the challenges presented.

Appendix A: Contributing Agencies

The following federal, state, and local public safety departments and agencies contributed to the creation and completion of this document. These contributions represent the combined opinions of experienced individuals in the field of ISSI and CSSI implementation.

- Bay Area Rapid Transit, Systems Engineering
- City of Chandler (Arizona) Police Department
- Connecticut Department of Emergency Services and Public Protection, Division of Statewide Emergency Telecommunications
- County of Los Angeles, Los Angeles Regional Interoperable Communications System
- East Bay Regional Communications System Authority
- Federal Bureau of Investigation
- Harris County, Texas, Public Safety Technology Services
- Indiana Integrated Public Safety Commission
- Missouri Department of Public Safety
- Montgomery County Hospital District (Texas)
- National Radio Operations Branch, Bureau of Land Management, Department of Interior
- New York Metropolitan Transit Authority Police Department
- Ohio Department of Administrative Services Multi-Agency Radio Communications System Program Office
- Oregon Department of Transportation, Wireless Communications Section
- State of Colorado, Governor's Office of Information Technology
- Texas Department of Public Safety

Appendix B: Best Practices Checklist

This appendix is meant to serve as a simple checklist of things to consider as agencies identify the "right" stakeholders to be involved in planning and implementation, assess and implement technology solutions, create policies, and plan ahead for maintenance and upgrades. It is meant to prompt practitioners to ask questions and consider strategic elements that may otherwise be overlooked.

STAKEHOLDERS

- ☐ Identify a diverse team of agency and partner agency leadership, radio systems provider personnel, and IP network professionals, as well as manufacturer personnel, consultants, technical experts, procurement professionals, and end users
- ☐ Engage non-technical personnel or individual champions to help secure funding from budgetary entities (e.g., state legislatures, city councils, county commissions, joint powers authorities) or promote educational campaigns to obtain community buy-in, as needed
- ☐ Conduct an inventory of available technical resources (e.g., knowledge, skills, abilities) to determine if you need to budget to hire adjunct personnel with a specific skill set or request that manufacturer provide certain knowledge/skills
- ☐ Engage the network professionals, engineers, or architects responsible for the IP-based network that serves as the backhaul connectivity for the ISSI implementation
- ☐ Include specific manufacturer personnel requirements (e.g., common titles, qualifications) in procurement and contractual documents to ensure the necessary support

TECHNOLOGY

- ☐ Conduct a full inventory of all current technology, including but not limited to, network paths, radio systems infrastructure, consoles, voice recorders, subscriber units, and software, hardware, and firmware versions and revision numbers
- ☐ Calculate the potential capital outlay required to either acquire replacement or new equipment, as well as estimated recurring O&M costs for network interconnection(s), software licensing, equipment, programming, training, and other services; add those anticipated recurring costs to proposed out year O&M budgets
- ☐ Define and agree upon compliance checking, both P25 Compliance Assessment Program - and procurement-driven, along with adequate interoperability testing with supplying manufacturers
- ☐ Confirm network accessibility and availability, as well as proper configuration of all network components (e.g., firewalls, servers, virtual private networks, latency timing)
- ☐ Identify current and expected loading requirements and any system constraints
- ☐ Find opportunities to collocate equipment at existing infrastructure sites with partnering agencies
- ☐ Articulate the approach to subscriber units on the system (e.g., specify select subscriber unit models)

- ☐ Develop a baseline understanding of what the P25 standards call for, which features the standards enable, and which decisions are left to the manufacturers and users directing the implementation

POLICY

- ☐ Craft shared operational policies for the use of the system(s) and the expected interactions among participating agencies
- ☐ Amend existing policies to include additional governance structures, as needed (e.g., IT governance)
- ☐ Define policies and procedures for initial and periodic training of all involved personnel from users to system administrators

THINKING AHEAD

- ☐ Ensure budgets consider any technology components that will lose warranty coverage during the budget cycle
- ☐ Consider adding a contingency element to capital and O&M budgets that can defray unforeseen costs that may arise and significantly impact the success of the implementation
- ☐ Discuss O&M costs among participating agencies to determine the appropriate cost sharing going forward
- ☐ Develop a maintenance plan that defines the overall maintenance processes, including roles and responsibilities of participating agencies
- ☐ Develop a comprehensive plan that identifies the process for system upgrades and software/hardware revisions over the anticipated life of the system including consideration for funding availability

Appendix C: References

1. International Wireless Communications Expo, "Exploring CSSI and ISSI," March 8, 2018.
2. Project 25 Technology Interest Group, Technology Benefits of P25, April 2016, **http://www.project25.org/index.php/documents/p25-whitepapers**.
3. Project 25 Technology Interest Group, "P25 Foundations: Applications and System Technology Updates for 2018," International Wireless Communications Expo, March 5, 2018, **http://www.project25.org/index.php/documents/ptig-p25-conference-presentations**.
4. Project 25 Technology Interest Group, "ISSI/CSSI Non-CAP Interoperability Testing Template," Version 2, updated January 17, 2019, **http://www.project25.org/index.php/compliance-assessment/p25-non-cap-issi-cssi-interoperability-testing**.
5. U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency, NCSWIC, *Inter RF Subsystem Interface Technology: Interconnecting Networks*, January 2015, **https://www.cisa.gov/publication/lmr-and-broadband-evolution**.
6. U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency, SAFECOM, and NCSWIC, *Project 25 Inter-RF Subsystem Interface (ISSI) and Console Subsystem Interface (CSSI) Primer*, January 2019, **https://www.cisa.gov/publication/p25**.
7. U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency, SAFECOM, and NCSWIC, *Best Practices for Planning and Implementation of P25 Inter-RF Subsystem Interface (ISSI) and Console Subsystem Interface (CSSI):Volume I*, January 2019, **https://www.cisa.gov/publication/p25**.
8. Wright, Scott. "Connecticut's P25 ISSI Applications." MissionCritical Communications. August 2019. Available online: **https://www.rrmediagroup.com/repository/files/SpecialReport-P25ISSIConnecticutlow-res.pdf**.