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

January 2019

SAFECOM®

Federal Partnership for Interoperable Communications

NCSWIC®

Preface

As the public safety community continues to recognize the importance of land mobile radio (LMR) operability and interoperability, the interest in Inter-RF Subsystem Interface (ISSI) technology has increased. This document specifically addresses the complex issues of planning for 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, 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 consider all aspects of planning, including partnerships and governance, identifying stakeholders, assessing technology, crafting and updating policies, and establishing operations and maintenance (O&M) requirements that may arise in a shared resources environment. This document focuses on suggested pre-planning and partnerships and governance elements; it provides best practices observed during these initial planning stages by local, county, regional, and state agencies implementing ISSI/CSSI. A second volume will cover the other planning components (e.g., stakeholders, technology, policies, O&M), as well as address various implementation best practices.

This document is a result of an extensive collaborative effort of the FPIC ISSI/CSSI Focus Group[1] whose membership is outlined in Appendix A.

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

Executive Summary

Project 25's (P25) open standards define features and functions and the interfaces of P25-compliant radio systems. Two of these interfaces, the Inter-RF Subsystem Interface (ISSI) and the Console Subsystem Interface (CSSI), are designed to enhance the operability and interoperability of new or existing land mobile radio systems. ISSI technology allows for multiple radio core systems or RF subsystems to link together and form larger wide-area networks, supporting the "system-of-systems" concept. The CSSI interface provides interoperability among multiple dispatch console vendors and system infrastructure manufacturers, which enables third party P25 console options.

Given increased interest in both ISSI and CSSI technology, the Federal Partnership for Interoperable Communications, supported by the Department of Homeland Security Cybersecurity and Infrastructure Security Agency Emergency Communications Division, established the ISSI/CSSI User Working Group (comprised of users and manufacturers) and the Focus Group (users only) to explore the ISSI/CSSI technology environment including but not limited to, successfully connecting single and multiple manufacturer ISSI or CSSI systems, collecting user and manufacturer implementation procedures, troubleshooting methods, and identifying best practices.

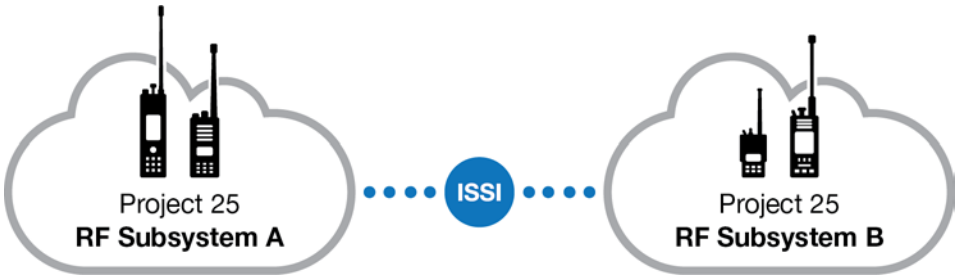
This document's purpose is to outline components for practitioners to consider when planning for and implementing an ISSI or CSSI implementation. The high-level components are rooted in best practices observed during all project phases by local, county, regional, and state agencies implementing ISSI/CSSI and are provided as a resource for others in the community who may be contemplating or implementing ISSI/CSSI. The six components are listed below; the first two are addressed in this volume while the other four will be addressed in a future volume.

- **Pre-Planning –** This component 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.
- **Partnerships and Governance –** Governance is one of the critical success elements that must be addressed to achieve and maintain a sophisticated interoperability solution. This component includes establishing trusted relationships, expressing a desire to interoperate, solidifying partnerships, and establishing formal governance structures.
- **Stakeholders –** It is critical to identify the "right" stakeholders to be involved in planning and implementation, including key leadership, radio personnel, network professionals, and end users.
- **Technology –** The selection and implementation of technological solutions and associated features and functions presents many potential challenges that public safety agencies should be prepared to address.
- **Policies –** Partnering agencies must establish standard operating procedures or policies to address everything from establishing talkgroups to group affiliation to software and hardware version control.
- **Thinking Ahead –** Throughout planning and implementation, agencies must constantly look forward and plan ahead for various elements, including acceptance testing, operations and maintenance, and future upgrades and feature implementations.

Background

Project 25 (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 land mobile radio (LMR) radio interoperability. As public safety radios transitioned from analog to digital technologies in the 1990s, and the implementation of trunked radio systems increased significantly, users sometimes found it difficult to 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 standards development, the Inter-RF Subsystem Interface (ISSI) provides a standardized, non-proprietary Internet Protocol (IP) connection of two or more P25-compliant trunked systems. These ISSI enabled radio cores or radio frequency subsystems (RFSS) may be from different vendors, 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 core or RFSS must incorporate an ISSI interface. In other words, ISSI technology allows for multiple radio core systems or RFSSs to link together and form larger wide-area networks, supporting the "system-of-systems" concept.

Figure 1. ISSI Example

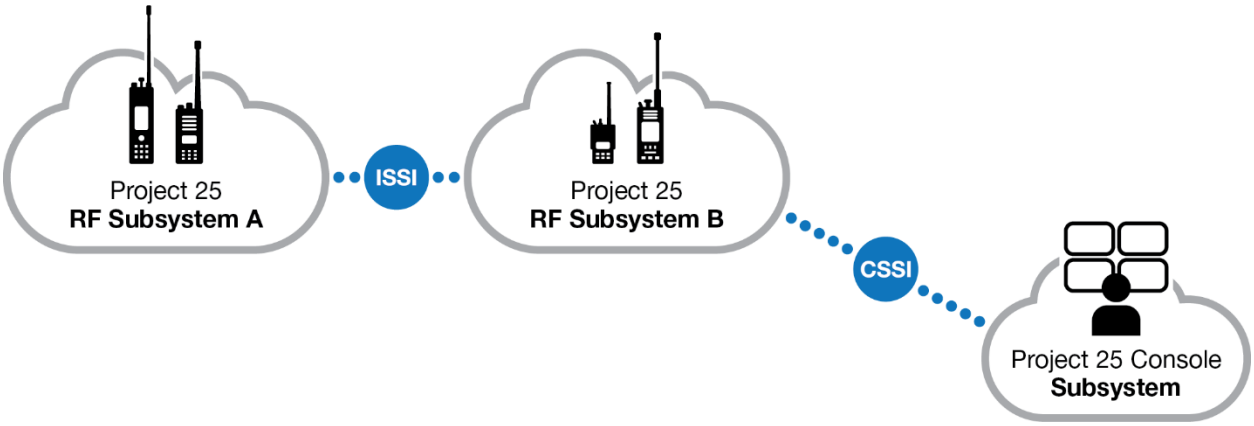


A system-of-systems approach relies on an agency's ability to own and manage an independent system while collaborating and sharing resources with other local, regional, state, tribal, and federal systems. Using a system-of-systems approach, each individual system becomes a component in an extended system, 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, identifying compatible technology and equipment, creating standard operating procedures, and designing and implementing 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, standard operating procedures, and recurring training, ISSI can be an invaluable 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 facilitate automatic aid scenarios among jurisdictions minimizing costly system resource expansions through the sharing of existing resources via ISSI connections.

The Console Subsystem Interface (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 limited choices for console system solutions. Each vendor had its own proprietary solution for connecting console equipment to the RFSS. As P25 moved toward digital IP connectivity, console systems had typically 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. This provides for interoperability between multiple dispatch console vendors 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.

Figure 2. CSSI Example



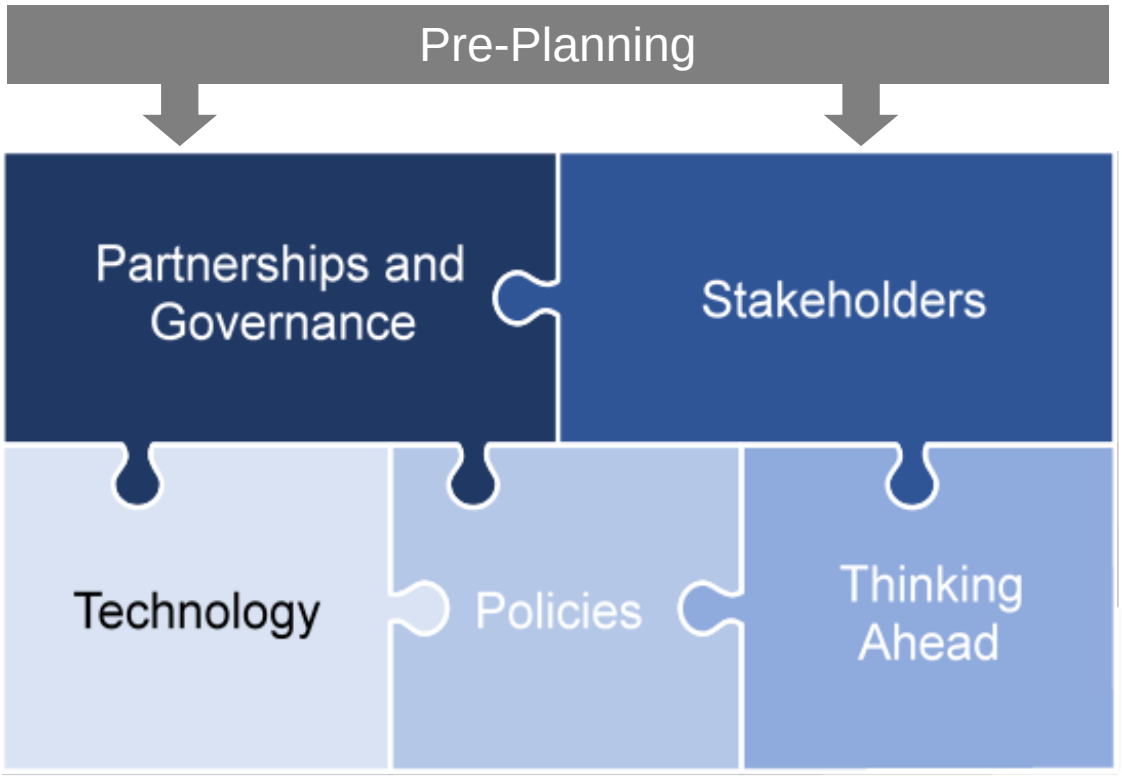
This document's purpose is to outline components for practitioners to consider when planning for and implementing an ISSI or CSSI. The high-level components are rooted in best practices observed during all project phases by local, county, regional, and state agencies implementing ISSI/CSSI and are provided as a resource for others in the community who may be contemplating or implementing ISSI/CSSI. The components as articulated are meant to prompt practitioners to ask questions and consider strategic elements that may otherwise be overlooked.

Planning Best Practices

The Federal Partnership for Interoperable Communications (FPIC)[2] ISSI/CSSI Focus Group has been discussing the challenges associated with ISSI and CSSI implementation and noted the need to share ISSI/CSSI best practices within the community to aid others in the planning and implementation processes. The Focus Group leveraged its combined experiences to identify six critical components of ISSI/CSSI planning and implementation as identified in Figure 3. Pre-planning is followed by a combination of establishing partnerships and governance, identifying the "right" stakeholders to be involved in planning and implementation, creating policies (e.g., standard operating procedures [SOP]), assessing and implementing technology solutions, and thinking ahead to plan for maintenance and upgrades. This volume specifically addresses pre-planning and partnerships and governance.

[2] 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.

Figure 3. ISSI/CSSI Planning Components



Pre-Planning

Pre-planning can include a nearly endless set of questions and topics to consider before planning and implementing an ISSI or CSSI. As with any technology project, initiating agencies must have internal dialogue regarding the feasibility, scope, and expected costs associated with an ISSI or CSSI implementation. In the case of ISSI, these conversations must also include potential partnering agencies regarding the project feasibility to establish a rough order of magnitude of potential costs, roles and responsibilities, purpose and application of ISSI/CSSI to preliminarily identified needs, and time schedules to effectively and efficiently move into the other planning phases. The Focus Group selected a handful of topics to address and identified specific best practices associated with each.

Purpose

It is important to understand the purpose and underlying motivation for pursuing ISSI connections to and from other stakeholders. Some agencies seek this solution, versus establishing a regional system, to maintain system ownership but still have interoperability with neighboring systems for mutual/automatic aid in response to planned and unplanned incidents. In Colorado, the ISSI "enables the respective agency to deploy a radio system from its preferred vendor rather than joining a statewide system, but at the same time honor its interoperability obligations by connecting to the statewide system via the ISSI."[3] Others leverage ISSI to extend coverage footprints using the RFSS resources of a neighboring agency. For example, one western city established an ISSI

[3] U.S. Department of Homeland Security, Office of Emergency Communications, *Emergency Communications Forum*, Volume 19, 2016, http://alaskalandmobileradio.org/pdf/DHS%20OEC%20ECF%20Volume%2019.pdf.

connection to extend radio coverage outside the city to the county jail, which is approximately 20 miles away. This provides an enhanced coverage solution that improves officer safety and negated the need for additional capital expenditures to add additional infrastructure to extend original system coverage.

Identifying Potential Partners and Setting Expectations

The initiating agency must identify potential partner agencies or jurisdictions that can help it achieve the desired outcome (e.g., improved interoperability, expanded coverage). That partner may be a neighboring jurisdiction or an existing system with overlapping coverage or a regional transportation agency with unique coverage needs.

An agency and its potential partners must understand and agree on what they want to interoperate, under what circumstances, for what purposes, and for which individuals or departments. The Focus Group indicated that the issues identified in Figure 4 are important to discuss first within an agency and then with potential partners to set and align expectations. It is important to note that any discussion of 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 thus the pre-planning must be considerate of the larger communications environment of all expected to be involved agencies.

Figure 4. Discussion Topics to Facilitate Expectation Setting

Discussion Topics
• Desired scope and extent of partnering agreements and envisioned governance structures • Magnitude of impacts of equipment, services, and personnel services to be committed and/or shared • Required key compatibilities, including estimated timelines to upgrade/implement CSSI/ISSI technology and the primary personnel and services needed to execute the project plan • Anticipated replacements of or updates to existing infrastructure and user equipment to accommodate ISSI/CSSI technology • Evaluation of existing system's capacity to guide appropriate dimensioning and expectation setting regarding features and functionalities of ISSI/CSSI with likely stakeholders • Estimated capital and recurring operations and maintenance (O&M) costs for network interconnection(s), software licensing, equipment, and services • Envisioned operational impacts, improvements, and desired outcomes • Methods and processes to gain initial "buy-in" from political leaders and identification of project champions

The Focus Group noted that a best practice – especially for agencies with previous ISSI experience and knowledge – is to develop a detailed list of requirements that address a potential partner agency's technical and administrative factors that would impact planning and implementation. One agency's such list includes, but is not limited to, the following:

- ✓ Foreign system must provide all interconnect circuits and maintain all circuits and associated costs
- ✓ Foreign system must have compliant software version to interconnect to home system
- ✓ Foreign system must be Phase II Time-division multiple access (TDMA)

- ✓ Foreign system and home system administrators will develop a technical/operations working group that will develop the following:
  - Define the quantity of users that will access ISSI
  - Define radio IDs of users that will access ISSI
  - Define and de-conflict IP address schemes of systems and user equipment
  - Define and agree to Rules of Use of the ISSI
  - Define foreign system site adjacency information for loading into foreign system CORE
  - Agree to use Advanced Encryption Standard (AES) 256 Encryption only.
  - Define and agree to P25 ISSI Standards to be included in system
- ✓ All parties will agree on the P25 ISSI standards to be tested and utilized
- ✓ All parties will agree to a common nomenclature for purposes of implementing the ISSI

Cost/Benefit Analysis

As alluded to in Figure 4 above, analyzing and cataloging the potential costs associated with an ISSI or CSSI implementation is a critical step. The Focus Group noted that a cost-benefit analysis must be understood by all potential participating agencies and their governing authorities. This analysis, at minimum, identifies capital costs, cost sharing opportunities, recurring costs, and expected O&M costs, as well as potential funding sources.

There is no "one size fits all" analysis as each agency or jurisdiction is different. Some will need to make significant hardware, software, and license expenditures, while others may only need software and licenses. Labor is an additional cost to consider for, among other activities, building and configuring circuits and testing. Other potential expenditures include outside consulting, networking, engineering, and similar services, as well as legal services associated with formalizing partnerships or governance. The other side of this equation – benefits – are intangible and thus difficult to quantify. In many cases, the benefits themselves are operational mandates or a desired end state (e.g., interoperability among field teams, implementing a regional interoperability plan, autoroaming to home system). Agencies and jurisdictions must do the best they can to summarize all potential costs and adequately articulate the anticipated benefits.

Education/Training

It is important to recognize that ISSI and CSSI are both complicated, albeit beneficial, solutions to public safety agency's communications challenges. The Focus Group's experience is such that each implementation is different; there are simply too many dependent variables ranging from network configurations to system software versions to subscriber unit firmware to manufacturer design decisions and accredited standards implementation choices. An agency considering an ISSI or CSSI implementation must recognize that there are many things "it does not know that it does not know." The agency must be willing to take steps to become a smart customer to mitigate later challenges.

The Focus Group noted a best practice is to attend prospective vendors' in-depth technical courses to develop a thorough understanding of what ISSI/CSSI enabled systems *can* and *cannot* do. If the P25 systems are already in place, agency personnel should attend training offered by the host system vendor, as well as the foreign system vendor (if different). Though this requires a monetary and time commitment on the agency's part, the knowledge gained is invaluable. Another best practice is to engage with a body, such as the FPIC ISSI/CSSI Focus Group, or directly with other jurisdictions that have similar ISSI configurations to understand what worked well, what did not

work well, and any specific challenges. The agency is then empowered to make informed decisions during a request for proposal (RFP) process, if relevant, and implementation.

Partnerships and Governance

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. 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.[4] A single entity cannot solve communications interoperability; rather, achieving interoperability requires a partnership among public safety/emergency response organizations across all levels of government.

The existing SAFECOM/National Council of Statewide Interoperability Coordinators (NCSWIC) *Emergency Communications Guide for State, Local, Tribal, and Territorial Officials* (Governance Guide) provides public safety professionals at all levels of government and disciplines a tool to assess, establish, and sustain effective emergency communications governance. This tool focuses on statewide, regional, or multi-jurisdictional governing bodies; however, many of the same principles apply to establishing governance or partnerships for ISSI or CSSI implementation, including documented authority, active membership, and rules of engagement.

Trust and a Desire to Interoperate

Agencies must engage in open and honest dialogue with potential partners to establish, build, and maintain trusted relationships. No matter the size or complexity of an ISSI implementation, trust among individuals and partner agencies is one of the most crucial elements to ensure success. In states or regions where local jurisdictions value and espouse independence and home rule, it may require multi-year trust building exercises combined with education of the potential benefits of ISSI connections to make progress. Building and maintaining trusted relationships requires sustained effort, persistent and active engagement, and potentially a different mindset for all parties involved. From planning to implementation to operation, there must be a shared understanding of everything from the proposed outcome to roles and responsibilities to SOPs that is rooted in the trusted relationships established among participating agencies to meet the shared communications operability and interoperability challenges.

Beyond trust, participating agencies must embrace a desire to interoperate. Agencies must "start early and talk often"[5] to solidify expectations and coordinate efforts. In Colorado, California, Virginia, and Oregon, the "willingness to collaborate among key stakeholders and a desire to improve interoperable communications"[6] drove the projects forward. Partners must be patient with one another; forcing a solution can damage trusted relationships and jeopardize desired outcomes. All parties must recognize and respect the bounds of what can and cannot be achieved through an ISSI implementation.

---

[4] U.S. Department of Homeland Security, SAFECOM, *Interoperability Continuum: A tool for improving emergency response communications and interoperability*, https://www.dhs.gov/sites/default/files/publications/interoperability_continuum_brochure_2_1.pdf.

[5] International Wireless Communications Expo, "Exploring CSSI and ISSI," March 8, 2018.

[6] U.S. Department of Homeland Security, Office of Emergency Communications, *Emergency Communications Forum*, Volume 19, 2016, http://alaskalandmobileradio.org/pdf/DHS%20OEC%20ECF%20Volume%2019.pdf.

Identifying Partners

As previously noted, the initiating agency must identify the partner agencies or jurisdictions that can help it achieve the desired outcome. Agencies can leverage existing venues, such as an existing Regional Planning Commission, to initiate ISSI discussions and gauge interest. For example, the Southern California Chapter of APCO, California Public-Safety Radio Association Chapter (Regional Planning Committee-5), is responsible for the regional 700 MHz plan and interoperability plan in the region. The like-minded and similarly skilled participants in these meetings and working groups originally broached the topic of ISSI connections in the region; they see ISSI as an opportunity to maintain their own communications systems while at the same time operate seamlessly among systems in the region, as needed. These parties are amid on-going discussions regarding potential ISSI connections.

Figure 5. Governance Bodies to Consider Engaging

Sample Governance Bodies
Consider leveraging existing governance bodies, such as: • Regional Planning Commission • Councils of Government • Radio Systems Operations Board • Joint Powers Authority • Board of Supervisors • Standing local, county, regional, or state interoperability committees (e.g., statewide interoperability executive committee, statewide interoperability governing body)

In the Washington, D.C., Maryland, and Virginia region, officials leveraged the existing, well-established Metropolitan Washington Council of Governments public safety committees and subcommittees (which includes fire chiefs, police chiefs, etc.) to identify and capture ISSI requirements. They will continue to leverage these groups to establish formal governance for ISSI management.

Understanding that each situation and governing body is different, public safety agencies should not have to start from scratch. There are many benefits to be gained from using an existing governance body to first identify partners and then plan ISSI or CSSI connections. Figure 5 identifies several governing bodies public safety agencies might consider engaging as it contemplates connecting P25 networks.

An existing governance body is likely already codified in law, may have administrative support (e.g., legal), and offers a broad array of potential partners beyond simply contemplating a connection with a neighboring agency. These elements could potentially save time, facilitate more robust or far-reaching solutions, and reduce frustrations for participating agencies. The existing body may also enhance future planning as ISSI/CSSI can be introduced into plans for other participating agencies. Finally, public safety agencies can leverage the body's established, trusted relationships; trust is a key element in the pursuit of complex technical solutions.

Governance Structure

To ensure that all participating agencies in an implementation remain aware and informed, it is important to use an agreed upon and workable governance arrangement selected by the stakeholder group. However, there is no "one size fits all" approach. The FPIC ISSI/CSSI Focus Group participants clearly demonstrated that every partnership is different and that governance structures should remain flexible to fit the given situation. The Focus Group also noted it is important to coordinate ISSI governance with existing system governance, management, and use, as relevant. As previously noted, the solution will not exist in a silo and thus the associated governance must be developed considering the existing communications environment.

Several agencies on the West Coast have found that small practitioner-level working groups of trusted personnel can successfully negotiate and establish connections among agencies. These groups of five to six individuals, limited to interested practitioners (e.g., police chiefs, fire chiefs) and radio network operations personnel, meet regularly to discuss opportunities, challenges, and functional activities. Agreements are solidified in legal documents and Memoranda of Understanding (MOU) are updated, as necessary, but it is these small, targeted groups that solidify the details, execute the agreements, and oversee the solution implementation.

Representatives from a western state noted it establishes intergovernmental agreements with each agency that chooses to connect to the State's P25 system via ISSI. These agreements cover the necessary topics ranging from purpose to compensation and warranties to termination. They also include exhibits or appendices that are functional in nature and cover mutual access governance and protocols, shared talkgroups properties and authorizations, and cooperation for enhanced operability.

As previously noted, the SAFECOM/NCSWIC Governance Guide provides recommendations and best practices to establish, assess, and update formal governance structures, as well as provides real-world examples. Consistent with the Governance Guide, a metropolitan law enforcement agency developed a charter and accompanying by-laws for a Regional Radio System Advisory Council. The documents include the key elements listed in Figure 6.

Figure 6. Formal Governance Documents

Document	Key Elements		
Charter	• Purpose • Responsibilities • Vision Statement • Mission Statement	• Membership • Officers • Meetings	• Decision-Making Procedures • Working Groups • By-Laws
By-Laws	• Name • Purpose • Responsibilities	• Members • Officers	• Board Meetings • Working Groups

It is important to note that this regional governing body was not established to manage the ISSI implementation but rather to manage the regional communications system once the connections are established. The ISSI implementation efforts are being coordinated by a small, practitioner-level working group, similar to the west coast public safety agencies. The metropolitan law enforcement agency is leveraging existing MOUs that allow it to establish small working teams to address issues. MOUs are an important part of governance structures because they define each party's roles and responsibilities, highlight the scope and authority of the agreement, clarify terms, and outline compliance issues. The Focus Group noted a best practice is to examine existing agreements to determine if the option exists to modify existing agreements to reflect the additional technical components and coordination required for an ISSI or CSSI implementation.

Figure 7 identifies additional items related to governance structure and format that should be incorporated into governance documentation.

Figure 7. Elements to Consider for Governance Documentation

Topic	Description
Roles and Responsibilities	Agreements should define roles and responsibilities for each participating agency and potentially individuals or technical teams from each participating agency.
Representation	It is worth considering that the representation required for project implementation may not be the appropriate team to drive continued operations and maintenance. One agency operating under a Joint Powers Authority agreement shared the board members who launched the project, negotiated and established relationships, drafted SOPs, and completed acquisition and deployment are not the appropriate personnel to manage on-going operations and maintenance or required technology refreshes. Agreements could address the need to assess representatives' skill sets at regular intervals to ensure the current team is adequately prepared to address the current lifecycle needs.
Meeting Participation	One organization operating under a Joint Powers Authority agreement emphasized the importance of keeping board members engaged. Complacency is a constant challenge. Governance documents can include language to address representatives' continued and active participation in the group's activities.
Updating Governance Documents	Agreements should include specific guidance to revisit the agreement language itself every three to five years to ensure the document, underlying agreement, technologies, and assigned parties are still relevant. A prescribed refresh can help prevent complacency and drive necessary discussions regarding upgrades or technology evolutions.
Financial / Budget Considerations	Agreements should address each participating agency's initial financial commitments and whether agencies will cost share, transfer funds, or split costs proportionally. It is important to note agencies' respective budget cycles, which can impact the funding availability and thus planning and implementation timelines. Documentation may also address the way agencies will handle future additions or modifications. One west coast public safety agency explained all participating agencies brought specific resources to the table to share (e.g., fiber, microwave links, tower sites, shelters) instead of cost sharing. Their documentation includes an annex that specifically defines the locations of shared assets and the nature of the sharing/collocation agreements.
Operational Commitments	Agreements should include a commitment to craft shared operational policies for the use of the system(s) and the expected interactions among participating agencies. This topic will be addressed in the ISSI/CSSI Best Practices Volume 2.

Other Agreements

The Focus Group noted the importance of examining existing or defining new agreements for other necessary components (e.g., backhaul). One agency shared that the local county, which is not a partner in the ISSI implementation, owns the microwave backhaul that it uses. The county currently charges no fees for the bandwidth; however, given that there is *not* an agreement in place, the county could abruptly implement fees that cripple the ISSI implementation. This example highlights the importance of formal agreements to protect agencies from changes.

Conclusion

ISSI and CSSI connections can greatly enhance emergency communications interoperability between different radio systems of the same or disparate manufacturers. Hundreds of ISSI and CSSI connections have been implemented across the country, allowing public safety agencies to extend their LMR networks, roam into neighboring communications systems while maintaining connectivity to their home systems, and seamlessly 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 due to the complexities of integrating this technology that has the potential to impact the core features and functionality of existing and new systems. While challenges can be formidable, the resulting enhancements to overall system operability and interoperability can be significant. If agencies leverage the best practices articulated here to thoroughly pre-plan and establish strong partnerships and formal governance, they 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
- 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, TX, 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
- 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 a single page checklist of things to consider as agencies work through pre-planning and partnerships and governance. It is meant to prompt practitioners to ask questions and consider strategic elements that may otherwise be overlooked.

Pre-Planning

- ☐ Clearly articulate the purpose and underlying motivation for pursuing ISSI connections to and from other stakeholders
- ☐ Identify potential partner agencies or jurisdictions and discuss what you want to interoperate, under what circumstances, for what purposes, and for which individuals or departments
- ☐ Develop a list of actual expectations and derived requirements that address a potential partner agency's technical and administrative factors that would impact planning and implementation
- ☐ Conduct a cost-benefit analysis, at minimum identifies capital costs, cost sharing opportunities, recurring costs, and expected O&M costs, as well as potential funding sources
- ☐ Attend vendors' in-depth technical courses to develop a thorough understanding of what ISSI/CSSI enabled systems can and cannot do
- ☐ Engage with a body, such as the FPIC ISSI/CSSI Focus Group, and/or directly with other agencies that have similar ISSI configurations to capture lessons learned and other best practices

Partnerships and Governance

- ☐ Reference the SAFECOM/National Council of Statewide Interoperability Coordinators *Emergency Communications Guide for State, Local, Tribal, and Territorial Officials*
- ☐ Engage in open and honest dialogue with potential partners to establish, build, and maintain trusted relationships
- ☐ Embrace a desire to interoperate and recognize and respect the bounds of what can and cannot be achieved through an ISSI implementation
- ☐ Leverage existing governance bodies, as appropriate, to identify potential partners
- ☐ Select partner agencies or jurisdictions and remain open and inclusive to partners joining later
- ☐ Establish an agreed upon and workable governance arrangement with the selected agencies
- ☐ Coordinate ISSI governance with existing system governance, management, and use, as relevant
- ☐ Examine existing agreements to determine if the option exists to modify existing agreements to reflect the technical components and coordination required for an ISSI/CSSI implementation
- ☐ Manage expectations regarding the technology to be implemented and the scope of the implementation project(s)
- ☐ Draft formal agreements (e.g., memoranda of understanding) and governing documents (e.g., charter, by-laws)
    - ☐ Define roles and responsibilities for each participating agency and potentially individuals or technical teams from each participating agency
    - ☐ Address the need to assess governance board members' skill sets at regular intervals to ensure the current team is adequately prepared to address the current lifecycle needs
    - ☐ Include language to address board members or representatives continued and active participation in the group's activities
    - ☐ Include language to revisit the agreement itself every three to five years to ensure the document, underlying agreements, technologies, and assigned parties are still relevant
    - ☐ Address each participating agency's initial and future financial commitments and whether agencies will cost share, transfer funds, or split costs proportionally
    - ☐ Include a commitment to craft shared operational policies for the use of the system(s) and the expected interactions among participating agencies

Appendix C: References

1. SAFECOM/NCSWIC, *Emergency Communications Guide for State, Local, Tribal, and Territorial Officials,* September 2015, https://www.dhs.gov/sites/default/files/publications/2015%20Governance%20Guide_Master_508c%20Final.pdf
2. U.S. Department of Homeland Security Office of Emergency Communications, NCSWIC, *Inter RF Subsystem Interface Technology: Interconnecting Networks*, January 2015, https://www.dhs.gov/sites/default/files/publications/ISSI-slicksheet-final-508_0.pdf
3. State of Oregon, *Interoperability Assessment and Plan Regarding: Major Trunked Radio Systems in Oregon*, April 6, 2017.
4. Metropolitan Washington Council of Governments, *Evolving Needs: Interoperable Communications and ISSI: Executive Brief*, Washington, D.C.: MWCOG.
5. Metropolitan Washington Council of Governments, *Evolving Needs: Interoperable Communications and ISSI: Technical Summary*, Washington, D.C.: MWCOG.
6. International Wireless Communications Expo, "Exploring CSSI and ISSI," March 8, 2018.
7. U.S. Department of Homeland Security, Office of Emergency Communications, *Emergency Communications Forum*, Volume 19, 2016, http://alaskalandmobileradio.org/pdf/DHS%20OEC%20ECF%20Volume%2019.pdf.
8. Project 25 Technology Interest Group, *Technology Benefits of P25*, April 2016, http://www.project25.org/index.php/documents/p25-whitepapers.
9. 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.
10. U.S. Department of Homeland Security, SAFECOM, *Interoperability Continuum: A tool for improving emergency response communications and interoperability*, https://www.dhs.gov/sites/default/files/publications/interoperability_continuum_brochure_2_1.pdf.