

SHARED COMMUNICATION SYSTEMS AND INFRASTRUCTURE (SCSI) FOR PUBLIC SAFETY COMMUNICATIONS

SCSI PROJECTS OFFER PUBLIC SAFETY ORGANIZATIONS THE CHANCE TO ENHANCE THEIR COMMUNICATIONS OPERABILITY AND INTEROPERABILITY BY SHARING INFRASTRUCTURE, CAPABILITIES, AND SERVICES IN SUPPORT OF THEIR MISSION CRITICAL FUNCTIONS.



DEFINING SCSI

Across the United States, public safety organizations continue to recognize the value of building communications networks that support multiple agencies and disciplines through SCSI.

SCSI benefits include, but are not limited to, the following:

- Increased operability and interoperability
- Improved spectrum use
- Optimized resource usage and management
- Streamlined intra-agency and interagency operations
- Decreased duplication of investmentsReduced capital and operations and
- maintenance (O&M) expenditures
- Positive environmental impacts
- Enhanced operational coordination and economies of scale

A SCSI approach encompasses the assets physical infrastructure (e.g., tower sites, facilities, repeaters, connectivity), real estate, spectrum, applications, subscriber units, and technical and operational staff—contributed in support of public safety communications.

A SCSI approach focuses on encouraging active resource sharing for organizations with national security, emergency preparedness, and public safety missions.

Once established, these systems can expand and grow to include other technologies, capabilities, and subscribers across all levels of government,¹ while employing and enhancing operability, interoperability, resiliency, and security.

SCSI efforts require coordination from all participating partners to ensure continued success. In particular, SCSI projects necessitate that stakeholders address a variety of governance, risk management, resource sharing, and operational considerations before and after implementation.



INITIATING AND/OR MAINTAINING A SCSI PROJECT

Maintaining siloed communications networks within the current "system of systems" results in inefficient and duplicative use of resources by agencies, which "often purchase and manage items in a fragmented and inefficient manner, [resulting] in duplication of effort...[and] significant costs."²

Organizations must take the following actions to ensure the success of the SCSI approach to supporting critical communication capabilities:

• **Governance.** Engage stakeholders across all levels of government to create and implement strong, inclusive, agile, and transparent decision-making processes

¹ Federal, state, local, tribal, and territorial agencies; private sector; and not-for-profit organizations that serve in a public safety, emergency management, or communications role.

² U.S. Government Accountability Office, "Improved Procurement of Land Mobile Radios Could Enhance Interoperability and Cut Costs," October 2016.

- *Risk management.* Develop a framework to address the risks, challenges, and concerns with implementing a SCSI approach
- **Resource sharing.** Identify available resources, decrease duplication of investment, and decrease capital and O&M expenditures/spending where possible and practical
- **Operations.** Develop methods to ensure secure operable and interoperable communications, streamlined intra-agency and interagency operations, and enhanced coordination among all participating entities



PREVIOUS SUCCESSES

SCSI projects continue to gain traction in the public safety community. Examples of such efforts include:

Puerto Rico (PR) and the U.S. Virgin Islands (USVI) Tactical Communications (TACCOM) Land Mobile Radio (LMR) Pilot 	The devastation of Hurricanes Irma and Maria created an opportunity to pursue a shared system environment in PR and the USVI. The PR/USVI TACCOM LMR Pilot will result in a robust LMR network supported by proper frequency management practices, comprehensive user education, effective site/repeater selection, and strong resiliency/security measures. This project created strong collaboration among federal participants.
Southwest Border Communications Working Group (SWBCWG) SCSI Project	The ability to effectively communicate along the nation's Southwest Border is a known challenge. In response, the SWBCWG is working to develop a report for decisionmakers outlining the governance, policy, resource sharing, and security considerations for implementing a SCSI project in the region. Partners include federal, state, local, and tribal government and public safety organizations operating along the border.
Statewide Systems	Many state networks already embrace SCSI tenets and have made great progress towards overcoming barriers to effective interjurisdictional and interstate communications. The SCSI approach provides them a resource for continued sharing, a path to resolve their collective challenges, and best practices for enhancing their shared systems.



NEXT STEPS

Multi-technology, cross-system, and cross-jurisdictional communications are essential needs for emergency responders in the 21st century. Public safety organizations can use a SCSI approach to enable: (1) effective implementation of available communications technologies and techniques; and (2) better utilization and integration of available communications assets in support of day-to-day operations and incident response.

In collaboration with the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA), public safety organizations should work to:

- Inspire SCSI membership by encouraging participation and engagement of additional partners
- Build leadership support for the effort by clearly articulating the need and direct involvement
- Promote user enthusiasm by relaying the benefits of this approach
- *Identify* evolving user needs, requirements, and resources that can be used in support of their projects
- Mitigate risks by articulating limitations and challenges, and suggesting solutions



TO FIND OUT MORE

For more information on the SCSI program, contact CISA's Public Safety & National Security and Emergency Preparedness Governance Branch, at **SCSI@cisa.dhs.gov**.