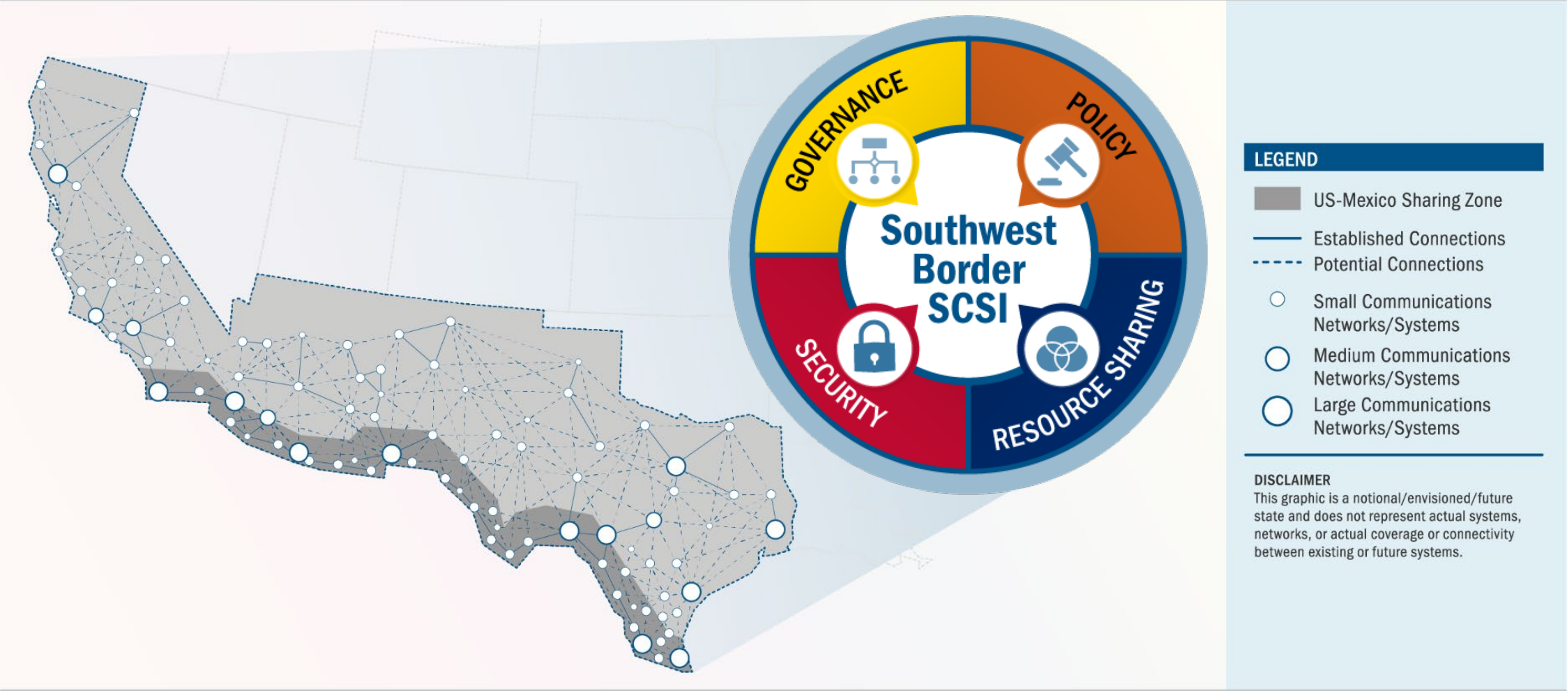


DISCLAIMER
This graphic is a notional/envisioned/future state and does not represent actual systems, networks, or actual coverage or connectivity between existing or future systems.

SCSI ALONG THE SOUTHWEST BORDER

DECEMBER 2019

Cybersecurity and Infrastructure Security Agency
Southwest Border Communications Working Group

EXECUTIVE SUMMARY

The objective of this report is to inform decision-makers and leadership across all levels of government[1] of the opportunities, challenges, and needed actions to create a Shared Communication Systems and Infrastructure (SCSI) project for federal, state, local, and tribal public safety organizations operating along the Southwest Border.[2]

Across the United States, public safety organizations[3] continue to recognize the value of building communications networks that support multiple agencies and disciplines through SCSI projects. Maintaining separate, siloed communications networks within the current “system of systems” results in inefficient usage and duplicative deployment of resources by agencies, which “often purchase and manage items in a fragmented and inefficient manner, [resulting] in duplication of effort…[and] significant costs.”[4] For example, if a responder from one jurisdiction was requested to provide assistance in another part of the state, the responder would be able to continue using their own radio due to the interoperability enabled by the SCSI approach. Current siloed systems may not interoperate, so the responder would need to obtain a new radio or pair with another responder from the home jurisdiction in the newly assigned location, resulting in delays.

Some of the current land mobile radio (LMR) systems in the Southwest Border region are well beyond their intended lifespans, having been in use for more than 20 years. Within this vast network of existing systems—all with varying levels of interconnection, interoperability, and owner types—rests the Southwest Border’s public safety communications infrastructure.

As outlined in the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency’s (CISA) Strategic Intent objective 2.3,[5] promoting resilient, secure, operable, and interoperable communications remains a top priority of the Federal Government. SCSI projects offer public safety organizations the opportunity to enhance their communications operability and interoperability by sharing infrastructure, capabilities, and services in support of their national security and emergency preparedness missions. To promote a shared communications environment along the Southwest Border, partners across all levels of government must identify available funding mechanisms and resources for the project. As such, ongoing capital, operations and maintenance (O&M), and sustainment investments are key to ensuring continual, secure, operable, interoperable, and resilient communications among partners in the region.

OBJECTIVE 2.3
EMERGENCY COMMUNICATIONS GOVERNANCE AND CAPACITY BUILDING

Responders at all levels of government have the ability to seamlessly share voice, video, and data communications during daily operations and major incidents and events.

Figure 1. DHS CISA Strategic Intent Objective 2.3

A Southwest Border SCSI project driven by active engagement of all partners in the region could lead to such benefits as lasting governance and technical solutions; improved operable and interoperable

[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] For the purposes of this document, the Southwest Border is defined as the terrestrial region within 110 kilometers (68.35 miles) of the U.S. and Mexico border, in line with the *Protocol Concerning the Use of the 806-901/935-940 MHz Bands for Land Mobile Services Along the Common Border* (1994 Protocol), which establishes the U.S. Mexico spectrum sharing zone as the region extending 110 kilometers from the border into both countries.

[3] The term *public safety* describes elements in the DHS Emergency Services Sector, which include law enforcement, fire and rescue services, emergency medical services, emergency management, and public works. For more information, see the DHS Emergency Services Sector website.

[4] U.S. Government Accountability Office, “Improved Procurement of Land Mobile Radios Could Enhance Interoperability and Cut Costs,” October 2016.

[5] DHS CISA, “Strategic Intent,” August 2019.

communications; streamlined intra-agency and interagency operations; and optimized resource use and risk management,[6] as outlined in Table 1.

Table 1. Southwest Border Communications Barriers and Potential SCSI Benefits

Communication Barrier	Potential SCSI Benefit
Outdated equipment	• Optimized resource usage and management • Improved currency of equipment software and firmware providing best operational, user experiences, and most up-to-date cyber protections
Deferred equipment maintenance	
Legacy approach to planning and operations	• Increased operability and interoperability • Improved and more efficient spectrum use • Modernized systems developed with joint technical expertise
Lack of current public safety or commercial communications infrastructure and capabilities	
Lack of access permissions for existing systems and networks (i.e., standardized agreements)	• Streamlined intra-agency and interagency operations • Ease of access to available operable and interoperable communications capabilities
Lack of technical resources (e.g., operators, specialists)	• Decreased duplication of investments • Reduced capital and O&M expenditures • More effective usage of existing finite and critical resources
Limited regional coordination	• Enhanced operational coordination and economies of scale • Positive environmental impacts

Though this document does not contain specific requirements for SCSI system design, maintenance, or operating procedures, it does detail the governance, policy, resource sharing, and security considerations that need to be addressed to successfully implement a regional SCSI project. Figure 2 provides a summary of the report's recommendations:

	Governance	**Policy**	**Resource Sharing**	**Security**
Recommendations	• Understand the current governance landscape • Build partnerships between public safety organizations at all levels of government • Agree on a governance model • Establish a governance structure • Implement collaborative and cross-regional coordination structures • Establish mechanisms to solve common communications project challenges, such as interoperability for data/voice and video	• Determine limitations in sharing funding • Establish templated SCSI baseline agreements • Harmonize legal interpretation of policies and regulations • Explore opportunities to streamline compliance with, and seek efficiencies for, environmental/historical preservation requirements • Consider opportunities to establish policies on resource delegation • Collaborate and develop an iterative risk management process	• Examine existing assets, identify gaps, and define the sharable assets and resources • Document resource sharing constraints, cost-sharing opportunities, and funding and sustainment mechanisms • Determine processes to evaluate system elements and other barriers for sharing • Develop a flexible sharing network to adopt potential changes as they occur • Address opportunities to test, evaluate, and integrate with new technologies and capabilities	• Develop a Security Plan that addresses both physical and cybersecurity: - Conduct vulnerability assessment(s) - Review current and unique threat environments - Account for varying security capabilities, standards, and requirements - Establish intended security, resiliency, and redundancy outcomes - Determine baseline security best practices • Implement the Security Plan

Figure 2. Report Recommendations Overview

As stated above, the intent of this report is to engage and inform public safety officials on the immediate need for a SCSI project in the region. The document may also serve as a reference for others as they seek to replicate this approach for other SCSI projects in other contexts or regions across the United States.

[6] For cybersecurity, risk is defined as the likelihood of a threat exploiting a vulnerability and the potential consequence or impact of that event. For financial purposes, risk is defined as the impact of such a threat and the cost to mitigate such threat.

Table of Contents

Tables

Figures

INTRODUCTION

The need for efficient and effective public safety communications across all levels of government is key for effective incident response. Emergency management and incident response activities rely on communications and information management systems that provide a common operating picture. The National Incident Management System (NIMS) is based on the concepts of interoperability, reliability, scalability, portability, and resiliency and redundancy of communications and information systems. However, responders operating in the U.S. Southwest Border region continue to experience challenges to establishing and maintaining adequate communications operability and interoperability.

Sharing resources and infrastructure across all levels of government is not new. Yet, because radio systems were originally designed, purchased, deployed, and operated as a single agency asset, the migration from viewing communication systems as a single agency asset to a resource that should be shared has been slow and hampered by antiquated laws and regulations.

In April 2019, members of the Southwest Border Communications Working Group (SWBCWG) [7,8] decided to establish the Southwest Border Shared Communication Systems and Infrastructure (SCSI) Focus Group to examine regional considerations necessary for establishing a SCSI project in the region. From these discussions, the focus group developed recommendations organized around four key themes: (1) governance; (2) policy; (3) resource sharing; and (4) security. This report intends to inform decision-makers and leadership across all levels of government on the SCSI concept and recommend the creation of a connected, interoperable network that leverages available "system of systems" technologies deployed in the region (e.g., land mobile radio [LMR], Long-Term Evolution [LTE], Wi-Fi, high frequency [HF] radio, microwave, wireline, satellite voice, video, Radio over Internet Protocol [RoIP], data communications systems) to improve communications for responders and the overall security of the Southwest Border.

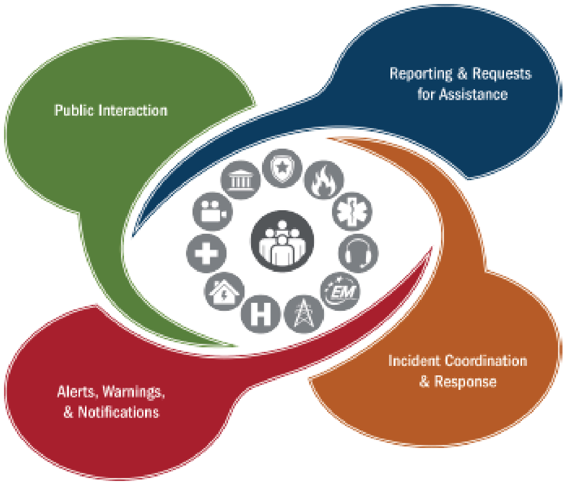

Public Interaction
Reporting & Requests for Assistance
Incident Coordination & Response
Alerts, Warnings, & Notifications
EM

Figure 3. Emergency Communications Ecosystem

Figure 3 depicts public safety stakeholders that contribute to the Emergency Communications Ecosystem, as described in the *National Emergency Communications Plan*.[9] These stakeholders participate in many types of communication, which include: (1) reporting and requests for assistance; (2) incident coordination and response; (3) alerts, warnings, and notifications; and (4) public interaction. For the purposes of this report, public safety is defined as the elements in the Department of Homeland Security (DHS) Emergency Services Sector, which include law enforcement, fire and rescue services, emergency medical services (EMS), emergency management, and public works.

[7] SWBCWG participants represent 10 federal offices, 20 state agencies, 66 local agencies, and six tribal nations "who rely on communications to support critical public safety and border security missions. Participants include stakeholders from various disciplines, including system managers, communications engineers and technicians, spectrum managers, emergency managers and planners, federal, state, local law enforcement, and fire, emergency medical services and management services officials and practitioners."

[8] Since 2008, the SWBCWG has supported the Southwest Border region's federal, state, local, and tribal efforts to establish, maintain and improve operable and interoperable public safety communications. The SWBCWG's efforts help ensure success in meeting end users' communications needs while improving coordination between U.S. departments and agencies at all levels of government.

[9] DHS Cybersecurity and Infrastructure Security Agency (CISA), "National Emergency Communications Plan," September 2019, 9.

Regional Communications Issues

Based on data gathered in a 2017 SWBCWG study, federal, state, local, and tribal (FSLT) public safety personnel operating along the border identified the following public safety communications issues as the most impactful on their operations:

- **Voice operability issues.** A lack of adequate funding across all levels of government presents challenges to effective communications operations. This limitation prevents the necessary: (1) critical communications in vast wilderness and rural areas along the border where little to no infrastructure or capabilities exist; (2) sufficient operations and maintenance (O&M) of current systems; and (3) periodic equipment and infrastructure upgrades required to gain access to existing shared channels, systems, or multi-agency, county, regional, or statewide networks. Many voice communications systems in the region are beyond their end-of-life.

- **Limited interoperability.** There are areas along the border with limited interoperability among and between public safety agencies at all levels of government. Until voice operability improves, interoperability will continue to suffer due to a lack of access to reliable communications equipment, infrastructure, and services. Interoperability is further challenged by the need for improved encryption services, operational coordination, system coverage, periodic repetitive training, and federal user integration into local, regional, and statewide systems. All respondents reported situations of “no interoperability” and insufficient operability of current voice and data systems.

- **Daily radio frequency (RF) interference.** U.S. public safety and governmental agencies in the region encounter RF interference caused by a lack of continuity in and appropriate regulation of the very high frequency (VHF) and ultra-high frequency (UHF) bands. Interference remains a daily challenge—peaking during critical agricultural seasons or events—and is complicated by a growing trend of re-sale and use of non-sanctioned second-hand subscriber units operating in Mexico using licensed U.S. channels. More specifically, RF interference continues to hinder timely incident response as current Federal Communications Commission (FCC) procedures do not provide immediate mitigations for interference, resulting in a regional perception of a lack of accountability and resolution of reported issues. Interference to critical systems, such as those located in El Paso, TX, San Diego, CA, or Tucson, AZ, could take days to resolve, leading to detrimental conditions for public safety.

- **Lack of region-wide wireless data.** Users reported significant gaps in both data operability and interoperability resulting from the lack of communications infrastructure in vast expanses of wilderness and rural areas along the border. The absence of wireless data availability places personnel at risk as they are unable to access and share essential information about emergencies, intelligence, trafficking, and criminal activity along the border. Enabling existing information resources and data repositories for wireless access and transmission remains a key component of promoting effective information sharing and improving the safety of public safety personnel operating contiguous to the international border.

Defining the SCSI Approach

The Southwest Border region requires reliable, resilient, connected, operable, and interoperable communications networks to support national security, emergency preparedness, and public safety missions. As a result, 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 these critical communications.[10] Once established, these systems may expand to include other technologies, capabilities, and subscribers across all levels of government, enhancing operability, interoperability, resiliency, and security.

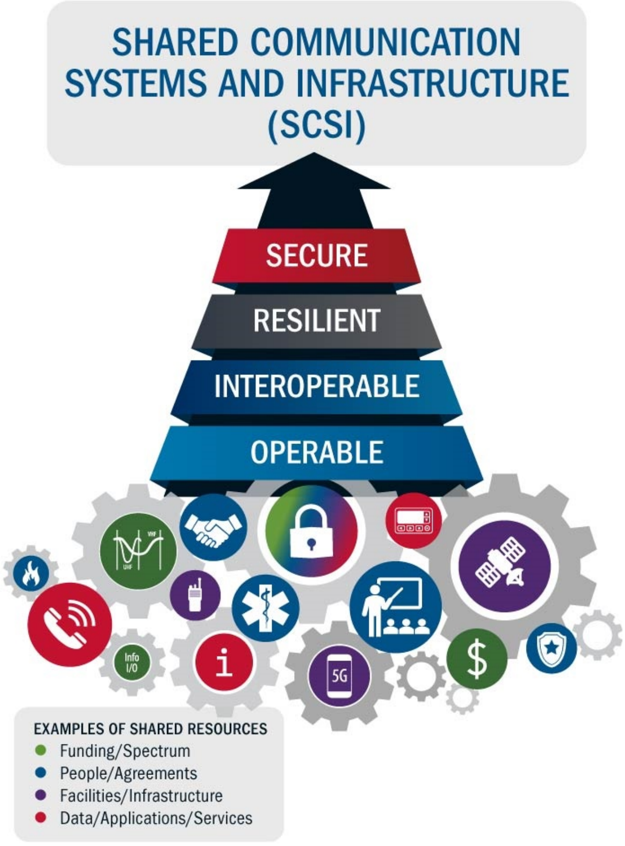

SHARED COMMUNICATION SYSTEMS AND INFRASTRUCTURE (SCSI)
SECURE
RESILIENT
INTEROPERABLE
OPERABLE
VHF
UHF
Info I/O
i
5G
$
EXAMPLES OF SHARED RESOURCES
● Funding/Spectrum
● People/Agreements
● Facilities/Infrastructure
● Data/Applications/Services

Figure 4. SCSI Overview

As a collaborative design effort, the Southwest Border SCSI project envisions a spectrally-efficient LMR network actively shared by FSLT users. This network's functionality may be augmented by Nationwide Public Safety Broadband Network (NPSBN) capabilities and potential infrastructure sharing through the First Responder Network Authority (FirstNet Authority) and other commercial broadband carriers focusing on public safety services. The network may also support further deployment or enhancement of the National Telecommunications and Information Administration (NTIA) law enforcement and incident response (LE/IR) dedicated interoperability channels (where appropriate), satellite capabilities, deployable assets, and other commercial network services offerings.

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

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

The Southwest Border SCSI project will result in a true "system of systems," focused on providing seamless Internet Protocol (IP)-based voice and data communications between telecommunicators in emergency communications centers (ECC)/public safety answering points (PSAP) and those responding public safety personnel in the field. To this end, the following sections includes a series of next steps for ensuring the development of a Southwest Border SCSI project that will enhance border security and overall public safety communications operations by creating a robust and survivable voice and data network for users.

[10] DHS CISA, "Shared Communication Systems and Infrastructure (SCSI) For Public Safety Factsheet," last accessed October 16, 2019.

GOVERNANCE

Key Potential Benefits – What's in it for Me?

- *Engages diverse stakeholders (e.g., government, non-governmental organizations [NGO], critical infrastructure/key resources [CI/KR] sectors, utilities, other public safety support elements)*
- *Strengthens existing relationships*
- *Establishes documented structure*
- *Facilitates transparent decision-making*

Strong governance is crucial to the success of any SCSI project. As defined in the *2018 Emergency Communications Governance Guide for State, Local, Tribal, and Territorial Officials* (2018 SLTT Governance Guide), "effective governance…facilitate[s] a greater understanding of existing communications capabilities and gaps, as well as the development of a coordinated strategic plan to prioritize resources, investments, and staffing….[resulting from] multi-disciplinary federal, state, tribal, regional, jurisdictional, and local entities working together to promote interoperability efforts."[11]

The Southwest Border SCSI project governance should work to identify viable public safety communications infrastructure components for shared use in the region. The associated Southwest Border SCSI project governance mechanisms should encompass the plans, policies, processes, and technical solutions needed to enhance communications operability, interoperability, security, and continuity, while encouraging active resource sharing. Governance of the Southwest Border SCSI project will need to clearly define project milestones and success metrics, determine decision-making structures, and outline ways to effectively assess and manage risks.

Identify All Partners

Governance represents a unified effort to coordinate the multiple functions that encompass emergency communications, to include the identification of project partners across all levels of government and related disciplines. The *National Emergency Communications Plan* describes a robust and reliable governance structure as one that "ensure[s] accountability, inclusiveness, adaptability, and action."[12] As such, governance of the Southwest Border SCSI project should focus on establishing inclusive, transparent decision-making processes by identifying all vested parties across levels of government (e.g., Statewide Interoperability Coordinators [SWIC], Statewide Interoperability Executive Committees [SIEC], communications systems managers, public safety agencies). More specifically, "establishing a shared vision, across jurisdictions and disciplines, and an effective organizational structure to support any project or initiative" will help clearly define participant roles and responsibilities, as well as "enhance interoperability by providing guidance…through common policies, processes, and procedures" for the shared network.[13] Inclusivity is key to the success of the Southwest Border SCSI project; therefore, identifying and encouraging participation from a variety of FSLT partners, as well as other public safety support elements,[14] is needed.

Account for Diverse Missions and Capabilities

The Southwest Border is a uniquely diverse region, with personnel operating in urban, rural, and wilderness areas. This SCSI effort should account for different missions and capability needs to ensure that the daily and incident (e.g., all-hazards, manmade, or natural) communications requirements of all partners are met. Examples of such mission sets include, but are not limited to:

- Border security;
- Border crime detection and suppression (e.g., drug and human-trafficking interdiction);

[11] SAFECOM/National Council of Statewide Interoperability Coordinators (NCSWIC), "Emergency Communications Governance Guide of State, Local, Tribal and Territorial Officials," 2018, 6.
[12] DHS CISA, "National Emergency Communications Plan," September 2019, 12.
[13] U.S. Government Accountability Office, "Improved Procurement of Land Mobile Radios Could Enhance Interoperability and Cut Costs," October 2016.
[14] For the purposes of the Southwest Border SCSI project, public safety support elements are defined as appropriate commercial entities, public and private utilities, transportation, CI/KR owners/operators, and NGOs.

- Rural and wilderness area emergency response (e.g., search and rescue, wildland fires, earthquakes, flash flooding);
- Suburban and urban public safety (e.g., law enforcement, fire prevention/suppression, EMS, emergency management);
- Maintenance of transportation and utility corridors;
- Wilderness area support, to include visitor engagement, resources/facility management, and search and rescue support (e.g., air-ground operations); and
- Quasi-public safety support or non-public safety public services communications (e.g., public works, traffic control, animal services, conservationists, biologists, tour guides)

Establish Inclusive Structures and Decision-Making Processes

SWBCWG members should account for partner perspectives by engaging a tiered governance structure that clearly defines efficient decision-making processes, while also incorporating lessons learned from existing regional shared infrastructure deployments to best meet evolving needs. At a minimum, this structure should include an Executive Board, a User Committee, and a Technical/Operational User Group to encourage active, balanced, and accountable membership, who will be responsible for establishing project timelines and milestones. The governance structure should also allow for the establishment of ad-hoc committees or working groups charged with investigating SCSI-related topics (e.g., interstate infrastructure sharing, spectrum licensing, systems access, enhancing interoperability between systems, cybersecurity challenges).

Sometimes oversight for a system evolves organically (e.g., handshake agreements) over many years or decades as resources become available. As a result, system governance may have also evolved organically, but strategic planning and official documentation (e.g., governance charters, by-laws, procedures) may not have accompanied these evolvements. For example, personnel changes (e.g., retirement, moving into new position) impact the oversight and governance of the system, ultimately resulting in reduced operational capability of that system and its users in accomplishing their missions. The SCSI project partners should ensure to capture and update all official documentations whenever a change to the governance structure or system occurs.

Recommendations

Based on the input received from regional partners and the guidance offered in the 2018 SLTT Governance Guide, project-specific governance recommendations include the following:

- **Understand the current governance landscape**, including how existing governance bodies coordinate communications and support operational sustainment functions (e.g., O&M, cybersecurity, public-private partnerships, training, exercises, evaluation programs) among participants.

- **Build partnerships** between public safety organizations at all levels of government—regardless of their department, agency, discipline, or jurisdiction—with the goal of formalizing cooperation through written agreements.

- **Agree on a governance model** that reflects unique organizational needs and potential partners from each element of the Emergency Communications Ecosystem. The Southwest Border SCSI governance model should be composed of FSLT entities supporting public safety missions in Arizona, California, New Mexico, and Texas.

- **Establish a governance structure** that can: (1) identify solutions to common governance, legal, fiscal, and technological challenges, such as interoperability for data, voice, and video; and (2) support a formal decision-making process through authorities, charters, bylaws, resolutions, and strategic plans. This governance body should focus on promoting active, inclusive user representation reflective of the unique requirements of all regional partners. The governance body will establish project timelines and milestones, and will maintain and capture updates to official oversight documentations when a change occurs.

- **Ensure coordination** with other governance groups to streamline communications lifecycle planning efforts, integrate emerging technologies, and implement lessons learned from existing regional shared deployments to meet evolving needs and priorities.

POLICY

Key Potential Benefits – What's in it for Me?

- *Modernizes funding and procurement*
- *Encourages legal compliance*
- *Supports consistent incident management*
- *Enhances citizen and responder safety*
- *Creates baseline agreements*
- *Improves spectrum usage consistency*
- *Promotes comprehensive risk management*

Establishing consistent policies to resolve communication barriers is another crucial component to a successful SCSI project. As highlighted in the 2017 SWBCWG report, the Southwest Border faces common challenges: (1) funding and procurement; (2) complying with regulations; (3) establishing baseline agreements; (4) optimizing spectrum usage; and (5) codifying risk management best practices. Any of these challenges could impede efforts to share existing communications infrastructure and assets among partners. As a result, the project will require a policy framework—or a set of detailed protocol, procedures, and guidance—to address these obstacles and support the project's vision and mission.

Streamline Funding and Procurement Processes

Multi-technology, cross-system, and cross-jurisdictional communications are an essential need for emergency responders in the 21st century. As demonstrated through the issuance of various Executive Orders and other Presidential decrees, this Administration is committed to ensuring the resilience and efficiency of the United States' national security and emergency communications infrastructure, as well as fortifying the associated information technology backbone and sharing resources where possible.[15,16,17,18,19]

Southwest Border SCSI partners may consider working with Congress to ensure federal investments can be used to enhance and upgrade non-federal infrastructure and services, supplementing gaps as they are identified.[20] As a result, partners along the border should identify policy changes to existing federal acquisition and procurement processes to allow federal funding to be used in support of non-federal communications infrastructure projects. These investments would reinforce interagency and interdisciplinary border security missions, improve emergency response, expand responder interoperability, and benefit all participating organizations.

Partners should also conduct legal reviews to determine whether there are state, local, and tribal regulations that prevent funding or existing infrastructure from being used as part of the SCSI project. The resulting policies should specify these limitations, while remaining flexible enough to adopt potential legislative changes as they occur.

[15] Exec. Order No. 13833, 83 F.R. 23345 (2018)

[16] Exec. Order No. 13807, 82 F.R. 40463 (2017)

[17] Exec. Order No. 13800, 82 F.R. 22391 (2017)

[18] Exec. Order No. 13768, 82 F.R. 8799 (2017)

[19] Developing a Sustainable Spectrum Strategy for America's Future, Daily Comp. Pres. Docs., 83 F.R. 54513 (October 25, 2018)

[20] The SCSI project offers opportunities to potentially modify language that is in United States Code 31, Section 1301, which outlines strict provisions as to how federal funds can be used to support infrastructure shared among federal and non-federal organizations. The law states that federal "appropriations shall be applied only to the objects for which the appropriations were made except as otherwise provided by law." This means that these funds cannot be used to purchase equipment or goods that will be owned by a non-federal entity unless there is clear congressional intent to use them for that purpose.

Harmonize Regulations and Identify Efficiencies

All levels of government are required to comply with zoning, environmental, real estate, and historical preservation, as well as security regulations, which can impact how a SCSI project is designed, built, and maintained. As organizations develop the Southwest Border SCSI project, increased engagement with land management agencies, Federal Preservation Officers, State Historic Preservation Officers, and Tribal Historical Preservation Officers, private sector CI/KR owners, and nonprofit organizations is highly recommended.

When considering new construction of, or colocation with, telecommunications infrastructure for the Southwest Border SCSI project, there may be opportunities to streamline compliance with Section 106 of the *National Historic Preservation Act*, and implementation of the provisions set forth in the *National Environmental Policy Act* via categorical exclusions or extraordinary circumstances, as appropriate. Project partners should also examine the *Wilderness Act of 1964* and any state historical and environmental policies to ensure compliance and seek additional opportunities to harmonize such regulations. Some project partners must also comply with varying levels of security requirements (e.g., the *Federal Information Security Management Act* [FISMA]). For further discussion on this, see the Security section in this report.

Establish Baseline SCSI Agreements

The SCSI project offers the opportunity to review existing regional systems agreements, revising them as necessary to clearly establish expectations, roles, and responsibilities for each SCSI participant. Memorandum of Agreement, Memorandum of Understanding, Interagency Agreements, Inter-Governmental Agreements, Joint-Use Agreements, Joint Powers Authorizations for the project should be modified to meet participant needs. For example, agreements should outline how partners will expedite review and approval to reduce communication barriers, respond and resolve disagreements, and promote resource efficiencies. Participants should utilize the project's governance mechanism to resolve differing legal perspectives between partner agencies.

Baseline project agreements, at a minimum, should address such topics as:

- How to actively engage with federal entities, tribal nations, state governors and legislatures, county commissions, mayors, and city councils in the region;
- Methods for evaluating existing systems' capacity, technical viability, and the associated cost for supporting additional users;
- A high-level overview of existing infrastructure, assets, O&M capabilities, services, plans, and spectrum usage for all SCSI partners;
- System evolution, succession planning, retirement of key personnel, high-level position changes; and
- Sharing security best practices and protocols.

Descriptions of foundational documentation and existing agreements and policies (e.g., charters, security procedures) may also be compiled and made available to all project partners via a centralized repository. Procedures regarding in-kind contributions (e.g., non-cash contributions such as property or third-party contributions including services, equipment, or property)[21], infrastructure maintenance, and upgrading components nearing end-of-life should be reviewed by legal teams to ensure adherence to existing rules, legislation, and regulations.

[21] Federal Emergency Management Agency, "What are In-Kind Contributions?" July 21, 2016.

Optimize Spectrum Usage

Non-federal public safety organizations must secure licenses from the FCC to operate their radio communications systems, meaning that these groups typically license frequencies from pool categories that are designated by the FCC for use only by entities with a public safety mission. Similarly, federal public safety entities receive their spectrum assignments from NTIA. As a result, non-federal and federal public safety radio communications systems often operate on different frequency bands or on different frequencies within the same band (e.g., VHF, UHF, 700 Megahertz [MHz], 800 MHz). FCC and NTIA rules, however, allow non-federal and federal entities to share their radio systems.

Due to the proximity to U.S. critical communications assets located along the Southwest Border, Mexico's adoption of the Asia-Pacific Telecommunity (APT) band plan for the 700 MHz band could impact both government and commercial services in the region as the U.S. and Mexico would operate under different and incompatible radio frequency bands in the 700 MHz spectrum.[22]

In a SCSI environment, organizations would be offered the opportunity to establish flexible policies, procedures, and protocols that delegate spectrum and other resources in a manner that can be replicated for similar efforts and allow for the inclusion of additional user groups based on valid mission need.[23] SCSI partners should also work with the FCC to meet additional licensing needs (e.g., licenses for backhaul, assignment of call signs, waivers to allow critical infrastructure entities to operate on public safety pool channels, waivers for public safety entities to operate on business pool channels).

Implement a Comprehensive Risk Management Framework

Similar to any project, the Southwest Border SCSI project may encounter various risks during its lifecycle, such as the loss of key staff or participants, loss of funding, bid protests, construction delays, frequency assignment problems, public protests, or challenges in local political environments. To best mitigate such risks, it is recommended that partners develop comprehensive risk management processes, codify best practices, and outline acceptable risk levels within formal agreements. The project should also incorporate risk management guidance from a wide collection of entities, such as the National Risk Management Center (NRMC),[24] to minimize overall risk impact to the effort.

Recommendations

Based on guidance and input from regional partners, project-specific policy recommendations include the following:

- **Determine limitations in sharing of available sustainment funding** to understand necessary changes to existing acquisition and procurement processes to ensure funds can be used in support of shared communications projects.
- **Establish baseline SCSI agreements** that are specific to the Southwest Border region, perform legal review to ensure adherence to existing laws and regulations, and develop a mechanism to resolve differing legal perspectives between partners.
- **Harmonize legal interpretation of Southwest Border SCSI-related policies and regulations** to promote sharing existing resources, infrastructure, and planned investments.

[22] SWBCWG has been monitoring this issue with the FCC for several years following Mexico's contemplation of moving to APT. The FCC, FirstNet Authority, and U.S. carriers are working to resolve interference issues.
[23] Arizona, California, and Texas have already signed a memorandum of understanding with the federal government for the use of the NTIA LE/IR channels.
[24] The NRMC works closely with the private sector and other key stakeholders in the critical infrastructure community to "Identify; Analyze; Prioritize; and Manage" the most strategic risks across the 16 critical infrastructure sectors. See the CISA National Risk Management website for more information.

- **Explore opportunities to streamline Southwest Border SCSI partner compliance with, and seek efficiencies for, environmental planning and historic preservation requirements** for infrastructure construction or planned modifications.

- **Identify opportunities to reduce the project's environmental impact and preserve environmental, historic, and cultural assets** in the region as a result of new construction or modification to existing assets.

- **Consider opportunities to establish flexible policies, procedures, and protocols that delegate resources in a manner that could be replicated** in similar efforts and allow for the inclusion of additional user groups based on valid mission need.

- **Collaborate and develop an iterative risk management process** based on existing resources (e.g., government frameworks, private industry guidance) that codifies best practices and acceptable risk levels within partner agreements.

RESOURCE SHARING

Key Potential Benefits – What's in it for Me?

- *Optimizes resource usage*
- *Decreases duplication of investments*
- *Reduces capital and O&M expenditures*
- *Enhances resiliency*
- *Improves cost containment*
- *Modernizes system components*
- *Decommissions outdated technology*
- *Provides advanced service delivery*

Resource sharing is essential to the success of any SCSI project. The Southwest Border SCSI project partners should consider shareable system assets (e.g., infrastructure, subscriber equipment, other operational components),[25] survey and catalog existing communications assets in the region, and identify capability gaps. Partners should also consider how resource sharing and integrating new technologies can: (1) mitigate risks posed by outdated equipment; and (2) address challenges posed by deferred equipment maintenance, a lack of technical resources, and insufficient staffing. Strong coordination and transparency between participants assist in identifying potential funding and resource sharing opportunities. In addition to identifying legal constraint to the sharing and funding, the SCSI project requires initial investment and sustainment capital and O&M funding (including expenditure for a technological refresh and required upgrades) for the entire system lifecycle.[26]

Consider Available Resources

In the Southwest Border region, the most common resources that could be considered in support of a SCSI project include:

- Infrastructure (e.g., towers, routers, repeaters, fiber, wireline, wireless, RF backhaul facilities);
- Spectrum (e.g., 700/800 MHz, UHF, VHF, microwave backhaul);
- Funding (e.g., grants, investments, budgeted sustainment funds);
- Public safety facilities (e.g., emergency operations centers, public safety communications centers, ECC/PSAP); and
- People, assets, and services (e.g., technologists, systems administrators, technical staff, shops or depots).

This infrastructure may be owned or leased by any federal, state, local, tribal, or private sector Southwest border SCSI participant with a public safety support mission. It is important to consider potential ways in which resources could be shared or utilized among users when planning for a SCSI project. As such, the

[25] DHS, "Emergency Communications System Lifecycle Planning Guide," May 2018,16.
[26] Ibid, ii.

current condition and lifecycle phase of assets may impact the "value" of resources, as well as the conditions under which the assets were originally purchased and deployed.

Survey Existing Assets and Gaps

Partners should develop a refined method to survey existing assets that can be brought forth in support of the project. Such an instrument should include ways to assess partners' inventories and provide clarity on resource sharing considerations for all entities on the system.

Until such a unified method is created, participants should collaborate with Arizona, California, New Mexico, and Texas' SWICs to identify and catalog existing regional assets and tools—such as the *Next Generation 911 (NG911) Maturity State Self-Assessment Tool*,[27] Geographic Information System (GIS) mapping tools, RF coverage analysis tools, and spectrum inventory tools—that can be shared in support of the project. Partners may benefit from considering methods for assessing current technology readiness within the Southwest Border operational area, including for those capabilities that are still considered emerging or next generation.

Successful training initiatives include:

- National Wildland Fire Training Apprenticeship Program for development of fire and aviation managers
- Interoperable Communications Technical Assistance Program for technical assistance, training, and resources
- Communications Unit Training Resources for NIMS and Communications Unit guidance

Once inventory is assessed, the SCSI project should determine what resources and coverage gaps exist (e.g., fiscal year funding gaps, cross-training of shared systems staff). Additionally, partners should identify any other technology, regulatory, or policy barriers that may impede successful resource sharing and review relevant findings with project partners. Best practices, as indicated by regional specialists and project partners, recommend streamlining decision-making processes for resource sharing based on observed gaps and barriers. This will likely result in an iterative negotiation process that may continue throughout the project's O&M phase as partnerships are established and expanded and new resource data emerges.

Establish Funding and Sustainment Mechanisms

As described in the *2018 Emergency Communications System Lifecycle Planning Guide* and summarized in Table 2, emergency communications systems, such as the one proposed for the Southwest Border SCSI project, include seven phases of implementation:[28]

Table 2. Emergency Communications System Project Planning Lifecycles

Emergency Communications System Project Planning Lifecycles	
Phase 1: Pre-Planning	• Inform and secure the decision to replace, upgrade, maintain, dispose of, or acquire a new system
Phase 2: Project Planning	• Formalize project team • Identify requirements • Develop the project plan
Phase 3: Request for Proposals and Acquisition	• Select the appropriate procurement vehicle • Procure systems and components
Phase 4: Implementation	• Develop an implementation plan • Install and test new systems • Train users • Transition from legacy to new systems and capabilities

[27] The *Self-Assessment Tool* is designed to help ECC/PSAP administrators and oversight personnel to evaluate their center's NG911 maturity state. Through a series of questions on NG911 governance, architecture, and security, the tool helps ECCs and PSAPs to strengthen their understanding of NG911 elements, increase their awareness of NG911 maturity continuum position, assist in planning NG911 transition steps, and enable a consistent terminology for the NG911 maturity level.

[28] DHS, "Emergency Communications System Lifecycle Planning Guide," May 2018, 3.

Emergency Communications System Project Planning Lifecycles	
Phase 5: Support, Maintenance, and Sustainment	• Inventory and maintain equipment • Manage budget • Assess and communicate needs
Phase 6: End of Lifecycle Assessment and Replacement	• Determine when to replace systems or components with solutions to best fit operational and technical needs
Phase 7: Disposition	• Determine options and dispose of legacy systems or components

Various types of communications infrastructure exist along the Southwest Border. As such, existing infrastructure varies in age and is impacted by a myriad of factors such as fiscal year funding cycles, continuing investments, maintenance activities and deferrals, obsolescence, and availability of parts and services. The age, lifecycle stage, and technical viability of infrastructure results in additional considerations for systems owners and operators regarding how, when, and what can be committed in support of this SCSI project. For example, regional prioritization approaches have successfully resulted in joint interoperable communications. Through those efforts, partners have been able to collaboratively prioritize investments nationally. Partners may consider similar prioritization schemes where regional stakeholders identify and target the greatest needs within the SCSI project's scope.

Working collaboratively, partners identify and document cost-sharing opportunities, in-kind contributions (e.g., capital infrastructure, spectrum, backhaul, tower sites, technical and operational staff), and additional funding methods available to the project. Table 3 provides a sample, non-comprehensive listing of SCSI project funding and sustainment mechanisms.

Table 3. Example SCSI Project Funding and Sustainment Mechanisms

Example SCSI Project Funding and Sustainment Mechanisms	
Capital Replacement Funding	• Organizations within a jurisdiction annually contribute operational, budgeted funding based upon levels of use to an upgrade/replacement fund to build reserves • As needs are identified for upgrade/replacement through capital budgeting processes, invested proceeds are used to meet capital budget expenditures
O&M Partnerships	• Participating organizations create an inter-agency field services organization (FSO) by accumulating technical, operational staff (e.g., system technicians, administrators, installers, programmers, repair depots), and equipment from existing agencies that will support the system following implementation • The FSO can operate as: (1) an independent enterprise entity supported by funding contributions from each participating organization; or (2) a unit or section of an existing organization that has service capabilities and equities in the major systems/project, funded by the participating agencies
Public-Private Partnerships	• Cost-sharing among government agencies, NGOs, and vendors • Private sector partners donate equipment (e.g., tower space, technical services, carrier services) • Public or private partners donate land, utility use, or access (e.g., Rights of Way [ROW], owned or leased/permitted property of land or structures) in compliance with governmental ROW requirements • Private sector partners are either: (1) paid one-time, flat "advance" fee for their services; (2) paid via device or network connection fees collected from the participating organizations; or (3) barter and trade services or offer co-location opportunities to benefit each other's operations

Integrate New Technologies and Capabilities

The Southwest Border SCSI project may also consider how to best integrate new technologies and capabilities to support the operability, interoperability, cybersecurity, and resiliency of shared public safety communications networks. Examples of emerging technologies that can be used in support of this SCSI network include:

- Internet of Things (IoT);

- IP-based mobile communications devices;
- Emergency Services IP Networks (ESInet);
- Priority telecommunications services;
- NPSBN and public safety offerings from other commercial carriers;
- Satellite capabilities and deployable assets;
- Commercial network service offerings;
- NG911 and next generation ECC/PSAP and
- Combined, co-located, and shared facilities supporting any of the above capabilities.

The ability to develop, test, and evaluate new technologies before deployment to ensure successful deployment, use, and compatibility with existing systems, while benefiting from economies of scale and minimizing duplication of effort and investment.

Recommendations

Based on guidance and input from regional partners, project-specific resource sharing recommendations include the following:

- **Examine existing emergency communications assets, identify gaps, and streamline decision-making processes for resources sharing** and maintain inventory of shareable and operationally-ready regional assets and resources.

- **Identify and document** resource sharing constraints, cost-sharing opportunities, in-kind contributions, and additional funding mechanisms.

- **Collaborate with project partners to determine** processes for evaluating system elements and other barriers for sharing.

- **Employ funding and sustainment best practices** to ensure longevity of SCSI project efforts.

- **Adopt a flexible sharing framework** so that SCSI participants pool resources and incorporate public safety support elements.

- **Be prepared for iterative resource sharing negotiations** as additional information on assets becomes available and new partners join the project.

- **Address opportunities to test, evaluate, and integrate with new technologies and capabilities** (e.g., IoT, NG911, NPSBN, other carriers' public safety broadband offerings) into the SCSI project.

SECURITY

Key Potential Benefits – What's in it for Me?

- *Implements comprehensive security plan that addresses physical security and cybersecurity*
- *Improves security of communication transport and content*
- *Streamlines intra-agency and interagency operations*
- *Bolsters physical security and cybersecurity posture*

Achieving resilient voice and data communications across the Southwest Border is essential for public safety agencies to execute their missions under any circumstances. SCSI project partners should ensure secure[29], operable, and interoperable communications while also remaining flexible and scalable.[30].The project has the potential to streamline interagency operations and enhance operational coordination in the region through standardization of security capabilities and requirements for project partners. These capabilities and requirements must address the current threat environments, which may include examples in Table 4:

Table 4. Example Security Threat Types and Descriptions

Threat Type	Description
Intrusion[31] (Unauthorized Data Access)	Attackers access sensitive databases (e.g., law enforcement, health records) to steal, modify, or corrupt the data.
RF Interference (Jamming)	Attackers unintentionally or intentionally interfere with Global Positioning Systems (GPS), radio, or other wireless system communications.
Malware	Designed and intended solely to damage or disable computers and computer systems and networks.
Ransomware	Malicious software designed and intended to block computer software systems until a sum of money is paid. For additional guidance, see *CISA's Insights on Ransomware*.
Supply Chain	Attackers infiltrate the supply chain and create backdoors to access intentionally vulnerable core processors and enable threat actor control of devices.
Telephony-Denial-of-Service Attack (TDoS)	Use of Voice over Internet Protocol (VoIP) systems to overwhelm phone systems rendering them incapable of placing or receiving calls.
Swatting	Manipulation of IP-based calls making the call seem as if it is originating from the location of a serious criminal act in-progress, prompting dispatch of a Special Weapons and Tactics (SWAT) team to the address.
Physical attacks	Damage and destruction of equipment and cables, unauthorized activation of shutoff switches, disruption of power supply, disruption of environmental control systems, or physical threats to personnel's health and well-being.

Develop Southwest Border SCSI Security Plan

To address these threats and beyond, partners should task security specialists with developing a SCSI project security plan for the region through the following steps:

1. Conduct vulnerability assessment(s)
2. Review current and unique threat environments
3. Establish intended security, resiliency, and redundancy outcomes
4. Determine physical security and cybersecurity best practices
5. Implement security plan

Conduct Vulnerability Assessment(s)

Southwest Border SCSI project partners should perform a vulnerability assessment (e.g., on user authentication, roles, responsibilities) to:

- Ascertain weaknesses;
- Identify applicable technical, physical security, and cybersecurity standards; and
- Establish and maintain a holistic security risk management program.

Key guidance, including applicable sections of the FISMA and other security policies or directives, should be considered for federal participation in the project. Project partners should also survey additional

[29] For purposes of this document, *secure* refers to the confidence in confidentiality, integrity, and availability of communications, to government sensitive or classified communications.
[30] For the purposes of this document, examples of *flexible* and *scalable* communications systems include, but are not limited to: (1) addressing secure voice and data in real time incident evolutions; (2) maintaining a security posture readily expandable for new or growing participation, evolving and incorporating new cyber practices; and (3) protections for new or expanding technologies.
[31] Intrusion threats include active intrusion into tactical communications networks of responders for the purposes of eavesdropping or providing false information to confuse or misdirect operations.

federal departmental requirements, non-federal, non-DHS policies, procedures, and protocols to ensure security robustness and resilience of the overall project.

Review Current and Unique Threat Environments

As threats continue to evolve and the attack surface expands, project partners should develop incident response plans and risk management strategies to compliment the security plan. Key tasks include:

- Identify new and evolving risks;
- Assess and prioritize risks;
- Develop and prioritize mitigation strategies based on cost-benefit analysis and other factors;
- Evaluate the impacts of mitigation implementation; and
- Develop an approach to detection and effective response and recovery procedures.

In addition, project partners should review existing best practices and develop new continuity of operations plans (e.g., disaster recovery plans and system failure plans that address how alternative communications paths would be established and utilized). Partners should also consider communications operability, interoperability, resiliency, and security with respect to third-party service level agreements and services from communications providers within those plans. Partners should collaborate with additional risk and threat management entities such as the NRMC to understand the cascading impact of threats.[32] The SCSI project should prioritize coordinating communications elements of all response and recovery efforts with the SWICs, major systems owners and operators, and other information technology or security administrators to maintain necessary security posture.

Establish Intended Security, Resiliency, and Redundancy Outcomes

Under the SCSI approach, the burden of maintaining system security no longer falls on a single organization. As a result, all participants share the responsibility of ensuring the physical security and cybersecurity of the SCSI project, while maintaining their own systems. The intended security, resiliency, and redundancy goals, associated responsibilities, and outcomes must be clearly defined and supported through policies, processes, and procedures aligned with current government and industry best practices (e.g., the *National Institute for Standards and Technology [NIST] Cybersecurity Framework*, International Organization for Standardization [ISO] 27001 Information Security Management, industry-accepted standards and guidelines). These outcomes should also account for the varying capabilities, standards, and requirements of all project partners in the region.

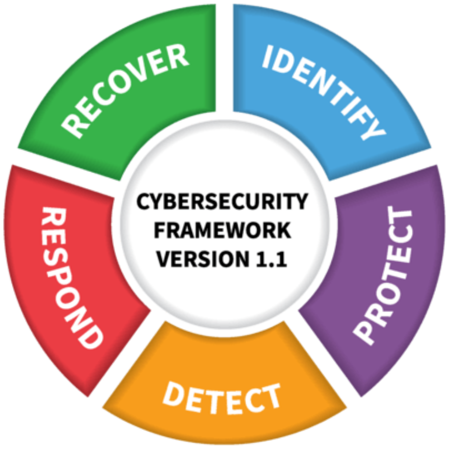


Figure 5. NIST Cybersecurity Framework

Determine Physical Security and Cybersecurity Best Practices

The SCSI project should determine and agree upon standardized physical security and cybersecurity best practices for all project partners. Based on baseline security requirements, all partners should have trusted connections or network-to-network protective interfaces between the partner systems. Partners should review existing best practices and requirements to ensure the finalized guidance is appropriate and applicable to the region. Partners should agree on standard physical security and cybersecurity best practices and minimums, acknowledging that stringent FSLT requirements remain aligned with the organization. Such practices should be inclusive of physical security and cybersecurity elements such as standardized information sharing, solution implementation, and measures to protect system components from physical threats. The SCSI project can also support the research and development of additional

[32] DHS, "National Risk Management Center," November 15, 2018.

physical security and cybersecurity best practices and maintain a working document that is reflective of all compiled project guidance. See Appendix B in this report for a list on SCSI project resources, including the following best practices:

Standardize encryption and information sharing best practices

Encryption is a crucial component to SCSI security as personally identifiable, investigative, sensitive, tactical, and other incident information are essential to public safety missions. The project partners should consider all applicable encryption requirements and standards and determine how encryption will impact interoperable voice and data communications. The presence of diverse public safety missions, different public safety support components, and non-public safety uses of the envisioned SCSI project will likely impact the method, manner, and types of encryption services to be used. Other considerations, such as processes for keying and regular rekeying, provision of over-the-air-rekeying, control, integration, interoperability, associated capital and O&M costs, and public access to information, should also impact the overall SCSI project encryption plan. Project partners should holistically consider encryption as a key security element requiring significant technical and operational coordination.

Consider Identity, Credential, and Access Management (ICAM) solutions

ICAM[33] is another consideration for SCSI security. Effective ICAM solutions should:

- Allow expression of data sharing and authentication requirements for all partners (e.g., agency bona fides, security, privacy, identity assurance, access control);
- Support consensus-based development of interoperable policy requirements (e.g., adoption of existing policies and frameworks: NIST Special Publications 800-53 and 800-63; adaption of existing policies within specific information sharing agreements);
- Provide the necessary tools to promote understanding of requirements for participating agencies (e.g., semantics, syntax, extension points); and
- Improve the ability to selectively authorize or deny access to resources at the individual, role, or organizational level.

Implement Security Plan

The SCSI project should implement the finalized security plan through a phased approach to ensure effective and unified adoption. All security guidance should be validated to ensure effectiveness for the overall project.

During implementation, partners should act on the results of decision-making processes, mitigation acceptance testing and evaluation planning, and coordination requirements for secure incident response and recovery. As the physical security and cybersecurity threat landscape continues to evolve, the SCSI project should routinely conduct vulnerability and risk assessments, monitor mitigation and recovery processes, and reassess and update the security plan.

Example Security Plan Element: Virtual Private Network (VPN)/Tunneling

Partners, like National Park Service (NPS), are using this method to share information in a secure and effective manner.

NPS establishes tunnels between systems and networks and manages them consistently to allow for the sharing and passing of data and communications.

VPNs are a form of tunneling that protect protected information system links using protocols like tunneling, security controls, and endpoint address translation to present the impression of a dedicated line.

Recommendations

Based on guidance and input from regional partners, project-specific security recommendations include the following:

[33] For additional information on ICAM, visit https://www.dhs.gov/safecom/icam-resources.

- **Develop a Southwest Border SCSI Security Plan** addressing both physical security and cybersecurity considerations of all project partners.
    - **Conduct vulnerability assessment(s)** and review current and unique threat environments which impact the project security plan.
    - **Review current and unique threat environments** and account for varying capabilities, standards, and requirements and establish intended security, resiliency, and redundancy outcomes from project partners.
    - **Establish intended security, resiliency, and redundancy outcomes** supported through policies, processes, and procedures aligned with current government and industry best practices (e.g., *NIST Cybersecurity Framework*).
    - **Determine physical security and cybersecurity best practices**, information sharing, and standardization for cybersecurity implementation within the SCSI project (e.g., interconnection security agreement, standard operating procedures, encryption standardization, ICAM solutions).
- **Implement the Southwest Border SCSI Security Plan** amongst all project partners through actionable measures such as decision-making process, mitigation acceptance testing and evaluation planning, and coordination requirements for incident response and recovery.

CONCLUSION AND PROPOSED NEXT STEPS

Implementation of a SCSI approach for public safety communications along the Southwest Border relies on two key factors:

- Modernization of existing emergency communications infrastructure, via near- and long-term continuous funding; and
- Partnership among FSLT agencies and their non-governmental counterparts.

A SCSI project results in the intentional coordination of all network owners and operators within the Emergency Communications Ecosystem, as well as greater efficiency and effectiveness in using limited resources. It is envisioned that NG911 will aggregate data from various sources to send it to those who need it most. FirstNet Authority's NPSBN and other broadband carriers will provide data and voice interoperability in support of LMR. In this environment, LMR will have converted transport and control of its sites to an all IP-based "system of systems." These various types of communications join in a larger interoperable network where public safety can readily use existing network resources where available, and augment where necessary.

The success of the Southwest Border SCSI project is contingent upon collaborative partners—across all levels of government—working together to identify and overcome challenges to effective system governance, policy, resource sharing, and security. In line with the recommendations presented in this report, partners operating in the region must work with their organizational leadership to ensure they can support the effective integration of available assets (e.g., spectrum sharing, site/repeater infrastructure selection, onsite staff/support) into a Southwest Border SCSI project.

In collaboration with DHS CISA, partners should continue to engage with regional public safety providers and policymakers to determine how the implementation of a Southwest Border SCSI project will result in: (1) effective implementation of available communications technologies and techniques (e.g., LMR and other capabilities) to address the public safety mission; (2) better utilization and integration of existing shared networks; and (3) identify funding and sustainment mechanisms.

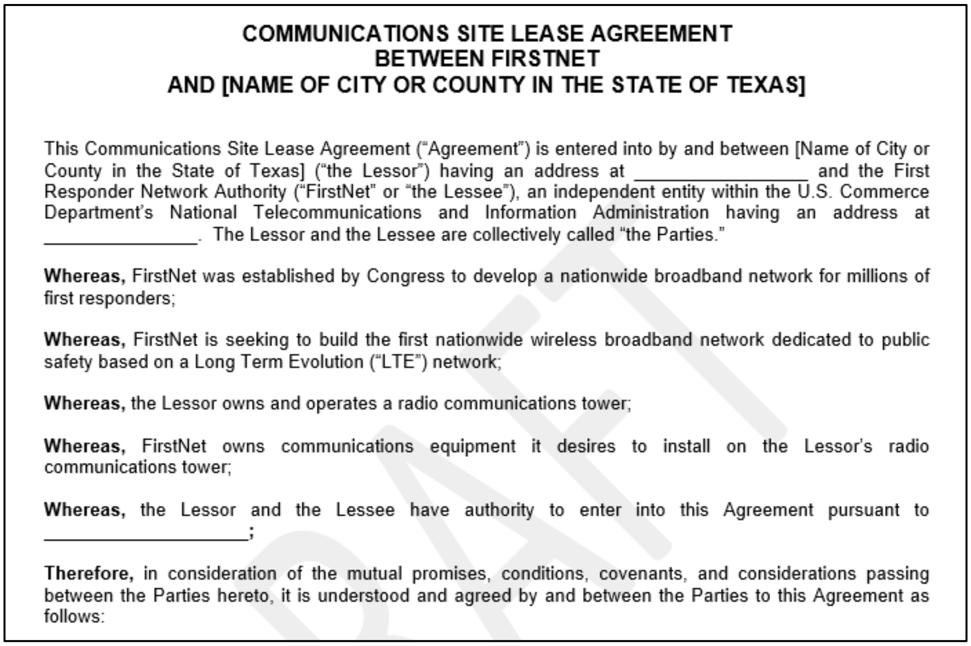
Decision-makers and interested parties are encouraged to dedicate time, effort, and resources to make progress on the recommendations from the governance, policy, resource sharing, and security sections of this report.

APPENDIX A: GUIDANCE ON WRITING MEMORANDUM OF UNDERSTANDING

To support the creation of baseline, templated Southwest Border Shared Communication Systems and Infrastructure (SCSI) project agreements, this appendix contains 10 suggested Memorandum of Understanding (MOU) sections for partner consideration. All proposed content is based on guidance in the Department of Homeland Security (DHS) and SAFECOM *Writing Guide for a Memorandum of Understanding*, which includes:[34]

1. **Introduction:** *Detail* the reason for the agreement
2. **Purpose:** *Discuss* the intention of the new or proposed capability that makes the agreement necessary and if applicable, compliant with regulatory guidance
3. **Scope:** *List* all project partners to be included in the agreement and *define* the relationships
4. **Definitions:** *Describe* the technical and operational terms associated with the capability or resource
5. **Policy:** *Outline* the circumstances under which the capability/resource can be used
6. **User Procedure Requirements:** *Identify* the agreement's obligations
7. **Maintenance:** *Specify* party or parties responsible for maintaining equipment, systems, and licenses associated with the capability/resource
8. **Oversight:** *Summarize* how the project partners will deploy or share the new capability/resource
9. **Responsibility for Policy, Procedure, or Protocol Compliance:** *Delegate* responsibilities to ensure all policies, procedures, or protocols related to the capability/resource are followed
10. **Update to the Agreement:** *Explain* how the agreement will be updated

Figures 6, 7, 8, and 9 provide additional example language from SWBCWG participating agencies:[35]



COMMUNICATIONS SITE LEASE AGREEMENT
BETWEEN FIRSTNET
AND [NAME OF CITY OR COUNTY IN THE STATE OF TEXAS]

This Communications Site Lease Agreement ("Agreement") is entered into by and between [Name of City or County in the State of Texas] ("the Lessor") having an address at ________________ and the First Responder Network Authority ("FirstNet" or "the Lessee"), an independent entity within the U.S. Commerce Department's National Telecommunications and Information Administration having an address at ________________. The Lessor and the Lessee are collectively called "the Parties."

Whereas, FirstNet was established by Congress to develop a nationwide broadband network for millions of first responders;

Whereas, FirstNet is seeking to build the first nationwide wireless broadband network dedicated to public safety based on a Long Term Evolution ("LTE") network;

Whereas, the Lessor owns and operates a radio communications tower;

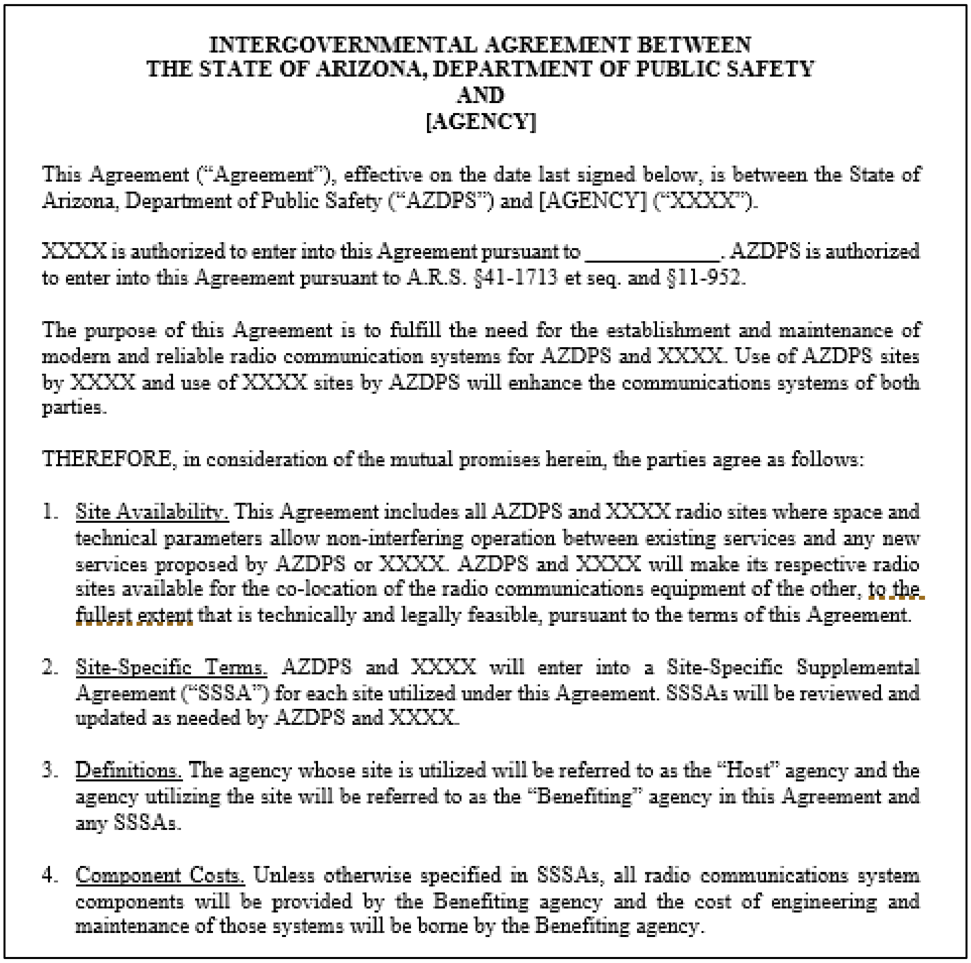
Whereas, FirstNet owns communications equipment it desires to install on the Lessor's radio communications tower;

Whereas, the Lessor and the Lessee have authority to enter into this Agreement pursuant to ____________________;

Therefore, in consideration of the mutual promises, conditions, covenants, and considerations passing between the Parties hereto, it is understood and agreed by and between the Parties to this Agreement as follows:

Figure 6. Draft Texas FirstNet Authority Communications Site Agreement Template

[34] DHS and SAFECOM, "Writing Guide for a Memorandum of Understanding," last accessed August 23, 2019.
[35] Complete MOU examples can be accessed at the SWBCWG Homeland Security Information Network website.



INTERGOVERNMENTAL AGREEMENT BETWEEN
THE STATE OF ARIZONA, DEPARTMENT OF PUBLIC SAFETY
AND
[AGENCY]

This Agreement ("Agreement"), effective on the date last signed below, is between the State of Arizona, Department of Public Safety ("AZDPS") and [AGENCY] ("XXXX").

XXXX is authorized to enter into this Agreement pursuant to ____________. AZDPS is authorized to enter into this Agreement pursuant to A.R.S. §41-1713 et seq. and §11-952.

The purpose of this Agreement is to fulfill the need for the establishment and maintenance of modern and reliable radio communication systems for AZDPS and XXXX. Use of AZDPS sites by XXXX and use of XXXX sites by AZDPS will enhance the communications systems of both parties.

THEREFORE, in consideration of the mutual promises herein, the parties agree as follows:

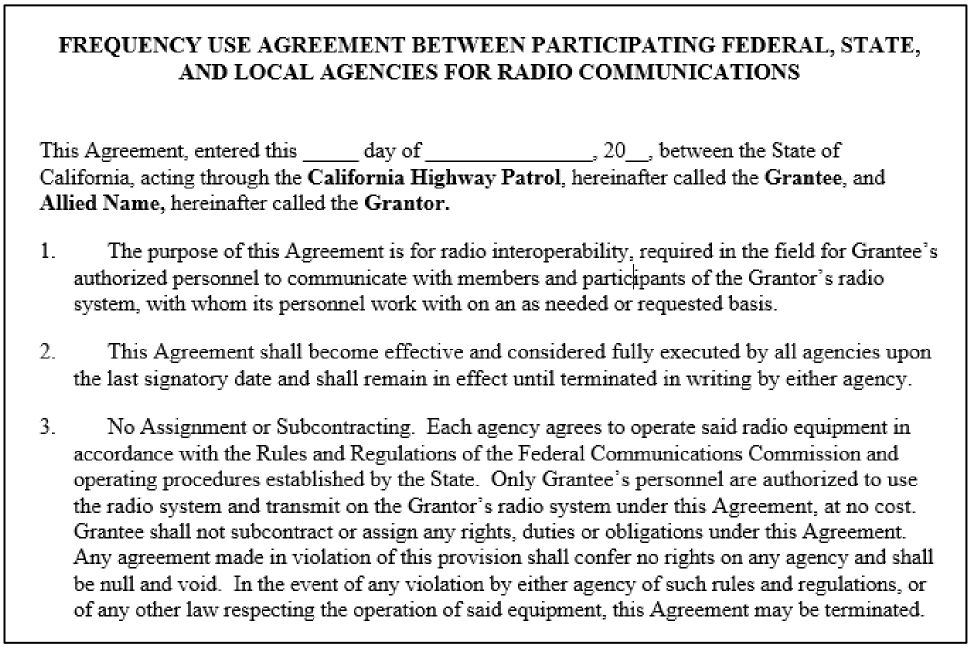
1. Site Availability. This Agreement includes all AZDPS and XXXX radio sites where space and technical parameters allow non-interfering operation between existing services and any new services proposed by AZDPS or XXXX. AZDPS and XXXX will make its respective radio sites available for the co-location of the radio communications equipment of the other, to the fullest extent that is technically and legally feasible, pursuant to the terms of this Agreement.

2. Site-Specific Terms. AZDPS and XXXX will enter into a Site-Specific Supplemental Agreement ("SSSA") for each site utilized under this Agreement. SSSAs will be reviewed and updated as needed by AZDPS and XXXX.

3. Definitions. The agency whose site is utilized will be referred to as the "Host" agency and the agency utilizing the site will be referred to as the "Benefiting" agency in this Agreement and any SSSAs.

4. Component Costs. Unless otherwise specified in SSSAs, all radio communications system components will be provided by the Benefiting agency and the cost of engineering and maintenance of those systems will be borne by the Benefiting agency.

Figure 7. Arizona Department of Public Safety Agreement Template



FREQUENCY USE AGREEMENT BETWEEN PARTICIPATING FEDERAL, STATE, AND LOCAL AGENCIES FOR RADIO COMMUNICATIONS

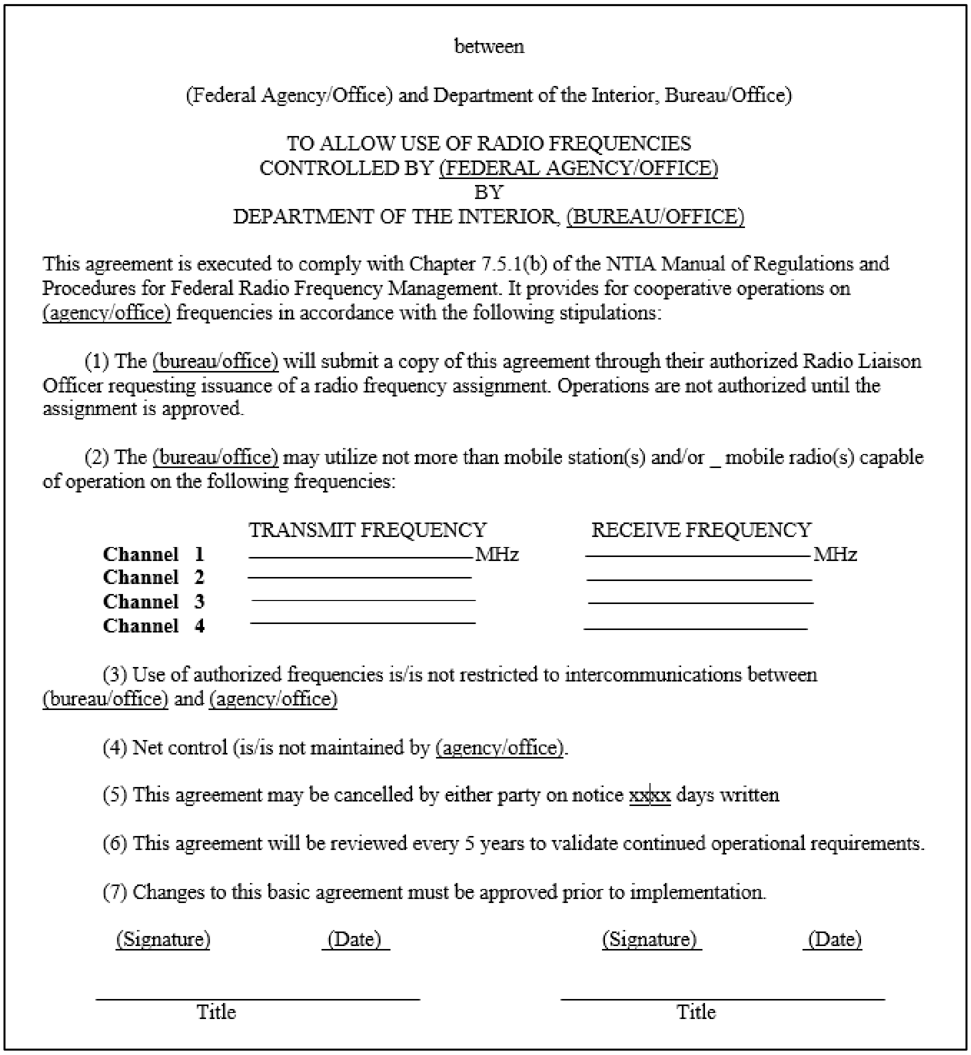
This Agreement, entered this _____ day of _______________, 20__, between the State of California, acting through the **California Highway Patrol**, hereinafter called the **Grantee**, and **Allied Name,** hereinafter called the **Grantor.**

1. The purpose of this Agreement is for radio interoperability, required in the field for Grantee's authorized personnel to communicate with members and participants of the Grantor's radio system, with whom its personnel work with on an as needed or requested basis.

2. This Agreement shall become effective and considered fully executed by all agencies upon the last signatory date and shall remain in effect until terminated in writing by either agency.

3. No Assignment or Subcontracting. Each agency agrees to operate said radio equipment in accordance with the Rules and Regulations of the Federal Communications Commission and operating procedures established by the State. Only Grantee's personnel are authorized to use the radio system and transmit on the Grantor's radio system under this Agreement, at no cost. Grantee shall not subcontract or assign any rights, duties or obligations under this Agreement. Any agreement made in violation of this provision shall confer no rights on any agency and shall be null and void. In the event of any violation by either agency of such rules and regulations, or of any other law respecting the operation of said equipment, this Agreement may be terminated.

Figure 8. California Highway Patrol Agreement Template



between

(Federal Agency/Office) and Department of the Interior, Bureau/Office)

TO ALLOW USE OF RADIO FREQUENCIES
CONTROLLED BY <u>(FEDERAL AGENCY/OFFICE)</u>
BY
DEPARTMENT OF THE INTERIOR, <u>(BUREAU/OFFICE)</u>

This agreement is executed to comply with Chapter 7.5.1(b) of the NTIA Manual of Regulations and Procedures for Federal Radio Frequency Management. It provides for cooperative operations on <u>(agency/office)</u> frequencies in accordance with the following stipulations:

(1) The <u>(bureau/office)</u> will submit a copy of this agreement through their authorized Radio Liaison Officer requesting issuance of a radio frequency assignment. Operations are not authorized until the assignment is approved.

(2) The <u>(bureau/office)</u> may utilize not more than mobile station(s) and/or _ mobile radio(s) capable of operation on the following frequencies:

	TRANSMIT FREQUENCY	RECEIVE FREQUENCY
Channel 1	____________________MHz	____________________MHz
Channel 2	____________________	____________________
Channel 3	____________________	____________________
Channel 4	____________________	____________________

(3) Use of authorized frequencies is/is not restricted to intercommunications between <u>(bureau/office)</u> and <u>(agency/office)</u>

(4) Net control (is/is not maintained by <u>(agency/office)</u>.

(5) This agreement may be cancelled by either party on notice <u>xxxx</u> days written

(6) This agreement will be reviewed every 5 years to validate continued operational requirements.

(7) Changes to this basic agreement must be approved prior to implementation.

<u>(Signature)</u> <u>(Date)</u> <u>(Signature)</u> <u>(Date)</u>

______________________________ ______________________________
Title Title

Figure 9. Department of the Interior Radio Frequency Agreement Template

APPENDIX B: ADDITIONAL SCSI PROJECT RESOURCES

This appendix contains a non-comprehensive list of publications, grouped by relevant subject, that provide additional information on topics related to sharing resources in support of interoperable communications along the Southwest Border.

PROGRAM BACKGROUND

- **Southwest Border Communications Working Group (SWBCWG)**
  The SWBCWG serves as a forum for federal, state, local, and tribal (FSLT) agencies in Arizona, California, New Mexico, and Texas to share information on common national security/emergency preparedness communications issues and collaborate on existing and planned activities in the region. This factsheet outlines the working group's efforts to enhance communications operability and interoperability, effectively use the region's available critical communications infrastructure resources, and ensure that programs continue to meet stakeholder needs.
  https://www.cisa.gov/international-cross-border-emergency-communications-efforts

- **Shared Communication Systems and Infrastructure (SCSI) For Public Safety Factsheet**
  The Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) developed this factsheet to act as a "101" guide for public safety organizations on the SCSI project approach. The factsheet introduces the SCSI concept, outlines key considerations, provides successful examples, and presents next steps for public safety organizations to consider when deploying the SCSI approach.
  https://www.cisa.gov/scsi

GOVERNANCE AND STANDARD OPERATING PROCEDURES (SOP)

- **2018 Emergency Communications Governance Guide for State, Local, Tribal, and Territorial (SLTT) Officials**
  The *2018 Emergency Communications Governance Guide for SLTT Officials* provides best practices for emergency communications officials to establish, assess, and update governance structures that represent all emergency communications capabilities (e.g., Land Mobile Radio [LMR], broadband, 911/Next Generation 911 [NG911], alerts and warnings).
  https://www.dhs.gov/safecom/governance

- **SAFECOM SOP Resources**
  The SAFECOM website provides resources to SLTT partners developing SOPs to support coordination of incident response and maintain interoperable communications. Resources include a template for creating a charter for a multi-agency communications committee.
  https://www.dhs.gov/safecom/sops

POLICY, AGREEMENTS, AND LIFECYCLE PLANNING

- **Writing Guide for a Memorandum for Understanding (MOU)**
  CISA and SAFECOM developed this guide to provide public safety stakeholders a recommended MOU structure and questions to consider when writing content.
  https://www.dhs.gov/safecom/governance

- **Funding Public Safety Communications Systems**
  SAFECOM and the National Council of Statewide Interoperability Coordinators (NCSWIC) developed this document to discuss funding mechanisms that have been used by states, territories, and localities to

support initial and sustained investments in public safety communications systems.
https://www.dhs.gov/safecom/funding

- **Fiscal Year 2019 SAFECOM Guidance on Emergency Communications Grants**
  CISA, in collaboration with SAFECOM and NCSWIC, developed this reference guide for entities applying for federal financial assistance for emergency communications projects. Updated annually, the guidance provides general information on eligible activities, technical standards, and other terms and conditions that are common to most federal emergency communications grants.
  https://www.dhs.gov/safecom/funding

- **2018 Emergency Communications System Lifecycle Planning Guide Compendium: Best Practices, Considerations, and Recommended Checklists**
  CISA, in collaboration SAFECOM and NCSWIC, developed this document to provide partners up-to-date information on public safety communications system lifecycle planning. These best practices are meant for stakeholders to use in their efforts to fund, plan, procure, implement, support, and maintain their systems, and eventually to replace and dispose of components.
  https://www.dhs.gov/safecom/funding

- **Emergency Communications Technical Assistance/Statewide Communication Interoperability Planning Guide**
  CISA's Interoperable Communications Technical Assistance Program (ICTAP) supports all 56 U.S. states and territories through development and delivery of training, tools, and on-site assistance to advance public safety interoperable communications capabilities. The guidebook presents ICTAP's service offerings including key topics such as coordinated statewide governance, comprehensive emergency communications planning, data operability and interoperability, and cybersecurity education and awareness.
  https://www.dhs.gov/publication/ictapscip-resources

TECHNOLOGY AND CYBERSECURITY

- **National Institute of Standards and Technology (NIST) Cybersecurity Framework**
  The NIST website includes an overview of the framework's purpose and phases, SLTT perspectives, success stories, online learning, and resources for managing cybersecurity-related risk (e.g., standards, guidelines, and best practices).
  https://www.nist.gov/cyberframework

- **CISA Cyber Resiliency Review (CRR)**
  The CRR is used to promote an organization's operational resilience and cybersecurity capabilities, enabling their ability to assess its capabilities relative to the NIST Cybersecurity Framework. The CRR seeks participation from a cross-functional team consisting of representatives from the business, operations, security, information technology, and maintenance areas within an organization.
  https://www.us-cert.gov/resources/assessments

- **United States Computer Emergency Readiness Team (US-CERT)**
  US-CERT collaborates with the global cybersecurity and critical infrastructure community in finding ways to protect the Nation's critical networks, systems, and assets. US-CERT provides an array of security resources for SLTT partners and offers such key services as risk and vulnerability assessments, operational planning and coordination, and incident response and recovery.
  https://www.us-cert.gov/

- **DHS SAFECOM Technology Resources**
  SAFECOM hosts several resources on a variety of public safety-specific technology topics, including: (1) alerts and warnings; (2) encryption; (3) interoperability; (4) LMR and broadband; (5) NG911; (6) Project 25; (7) communications resiliency; and (8) 5G, Internet of Things (IoT), and Smart Cities.
  https://www.dhs.gov/technology

- **DHS Cybersecurity Services Catalog for SLTT Governments**
  The catalog informs the SLTT community of available cybersecurity services that can promote the protection of their systems. All program, tools, and capabilities featured in this catalog are voluntary, non-binding, no cost, and available to stakeholders upon request.
  https://www.us-cert.gov/sites/default/files/c3vp/sltt/SLTT_Hands_On_Support.pdf

- **Multi-State Information Sharing and Analysis Center (MS-ISAC)**
  The MS-ISAC is a membership-based security organization focused on improving the cybersecurity posture of SLTT governments by acting as a focal point for cyber threat prevention, protection, response, and recovery. Membership services include, but are not limited to, incident response, cybersecurity advisories and notifications, and access to table-top cybersecurity exercises.
  https://www.cisecurity.org/ms-isac/

APPENDIX C: ACRONYMS

Acronym	Definition
APT	Asia-Pacific Telecommunity
CI/KR	Critical Infrastructure/Key Resources
CISA	Cybersecurity and Infrastructure Security Agency
CRR	Cyber Resiliency Review
DHS	Department of Homeland Security
ECC	Emergency Communications Center
EMS	Emergency Medical Service
ESInet	Emergency Services Internet Protocol Network
FCC	Federal Communications Commission
FirstNet Authority	First Responder Network Authority
FISMA	Federal Information Security Management Act
FSLT	Federal, State, Local, and Tribal
FSO	Field Services Organization
GIS	Geographic Information System
GPS	Global Positioning System
HF	High Frequency
ICAM	Identity, Credential, and Access Management
ICTAP	Interoperable Communications Technical Assistance Program
IoT	Internet of Things
IP	Internet Protocol
ISO	International Organization for Standardization
LE/IR	Law Enforcement/Incident Response
LMR	Land Mobile Radio
LTE	Long-Term Evolution
MHz	Megahertz
MOU	Memorandum of Understanding
MS-ISAC	Multi-State Information Sharing and Analysis Center
NCSWIC	National Council of Statewide Interoperability Coordinators
NG911	Next Generation 911
NIMS	National Incident Management System
NGO	Non-Governmental Organization
NIST	National Institute of Standards and Technology
NPS	National Park Service
NPSBN	Nationwide Public Safety Broadband Network
NRMC	National Risk Management Center
NTIA	National Telecommunications and Information Administration
O&M	Operations and Maintenance
OTAR	Over-the-air Rekeying
PSAP	Public Safety Answering Point
RF	Radio Frequency
RoIP	Radio over Internet Protocol
ROW	Right of Way

Acronym	Definition
SCSI	Shared Communication Systems and Infrastructure
SIEC	Statewide Interoperability Executive Committees
SLTT	State, Local, Tribal, and Territorial
SOP	Standard Operating Procedure
SWAT	Special Weapons and Tactics
SWBCWG	Southwest Border Communications Working Group
SWIC	Statewide Interoperability Coordinator
TDoS	Telephony-Denial-of-Service
UHF	Ultra-High Frequency
US-CERT	United States Computer Emergency Readiness Team
VHF	Very High Frequency
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network