SCIP Overview Guide

THE VALUE AND PURPOSE OF THE SCIP WORKSHOP

Every year the Department of Homeland Security (DHS) releases the Homeland Security Grant Program (HSGP) Notice of Funding Opportunity (NOFO) through the Federal Emergency Management Agency (FEMA) to announce funding opportunities that are available to states, territories, urban areas, and other local and tribal governments. These are DHS grants administered by FEMA with inputs from all elements of the homeland security enterprise. The new guidance addresses several recommendations advocated by the emergency communications community. DHS seeks to enhance the ability of states, local governments, tribes, and territories to prevent, protect against, respond to, and recover from potential terrorist acts and other hazards. To meet this requirement, states and territories are required to have an approved Statewide Communication Interoperability Plan (SCIP).

A SCIP defines the strategic direction for interoperable and emergency communications within a state. It outlines interoperability goals with specific steps for action (including action owners and completion timeframes) and defined mechanisms to measure achievements. The state may use the SCIP to demonstrate to leadership and elected officials' statewide successes, outline obstacles or challenges, and report on progress. The SCIP provides structure and focus through strategic planning for a one to three-year timeframe. It supports states and territories in developing their vision of future capabilities by incorporating all elements across the Emergency Communications Ecosystem.

CISA partnered with the National Council of Statewide Interoperability Coordinators (NCSWIC) to develop the State Interoperability Markers, which are 25 indicators of interoperable communications maturity aligned with the Interoperability Continuum, used to identify interoperability strengths and gaps, and then leveraging that information to set strategic goals in their SCIPs, and inform TA requests.

In June 2019, Cybersecurity and Infrastructure Security Agency (CISA) began self-assessment workshops, which allowed states to collaborate regionally while assessing their individual status against newly developed State Interoperability Markers. The information collected will enable CISA to tailor support through technical assistance (TA) to states and territories, enhancing their interoperable communications capabilities. This has allowed states to continue the discussion of needed action within the realm of emergency communications, and ensure they plan and successfully implement interoperability solutions.

EMERGENCY COMMUNICATIONS PLANNING FRAMEWORK

There are several different emergency communications frameworks states and territories can use to outline their goals and objectives. The Interoperability Continuum has five lanes: Governance, Standard Operating Procedures, Technology, Training & Exercises, and Usage.

Interoperability Continuum

*Governance		Individual Agencies Working Independently	Agencies Informally Coordinating	Key, Multi-Disciplinary Staff Collaborating on a Regular Basis	Regional Committees Working within a Statewide Communications Interoperability Plan Framework	Multi-State Consortiums that Routinely Coordinate and Collaborate	Federal Participation and Coordination at All Levels of Government on a Routine Basis
SOPs/SOGs and FOGs		Individual Agency SOPs/SOGs and FOGs		Joint SOPs/SOGs and FOGs for Events and Incidents	Regional Set of Communications SOPs/SOGs and FOGs		National Incident Management System Integrated SOPs/SOGs and FOGs
Technology	Data Elements	Swap Files	Common Applications	Custom-Interfaced Applications	One-Way, Standards-Based Sharing	Two-Way, Standards-Based Sharing	
	Security & Continuity of Operations	Inventory and Management of Physical and Software Assets, Personnel, and Access Levels	Routine Threat, Risk, and Vulnerability Assessments	Develop and Implement Security and Cybersecurity Protocols	Proactive Security and Continuous Monitoring Capabilities	Regular and Sustained Security and Cybersecurity Capabilities	Effective Response, Mitigation, and Support Recovery Capability in Place
	Voice Elements	Swap Radios	Gateway	Shared Channels	Proprietary Shared System	Standards-Based Shared System	
Training & Exercises		General Orientation on Equipment and Applications	Single Agency Tabletop Exercises for Key Field and Support Staff	Multi-Agency Tabletop Exercises for Key Field and Support Staff		Multi-Agency Functional Exercises Involving All Staff	Regular Comprehensive, Region-wide Training and Exercises
Usage		Planned Events	Localized Emergency Incidents		Regional Incident Management		Inter-Jurisdictional and Inter-Disciplinary Daily Use throughout Region

Left axis: Limited Leadership, Planning, and Collaboration among Areas with Minimal Investment in the Sustainability of Systems and Documentation

Right axis: High Degree of Leadership, Planning, and Collaboration among Areas with Commitment to and Investment in the Sustainability of Systems and Documentation
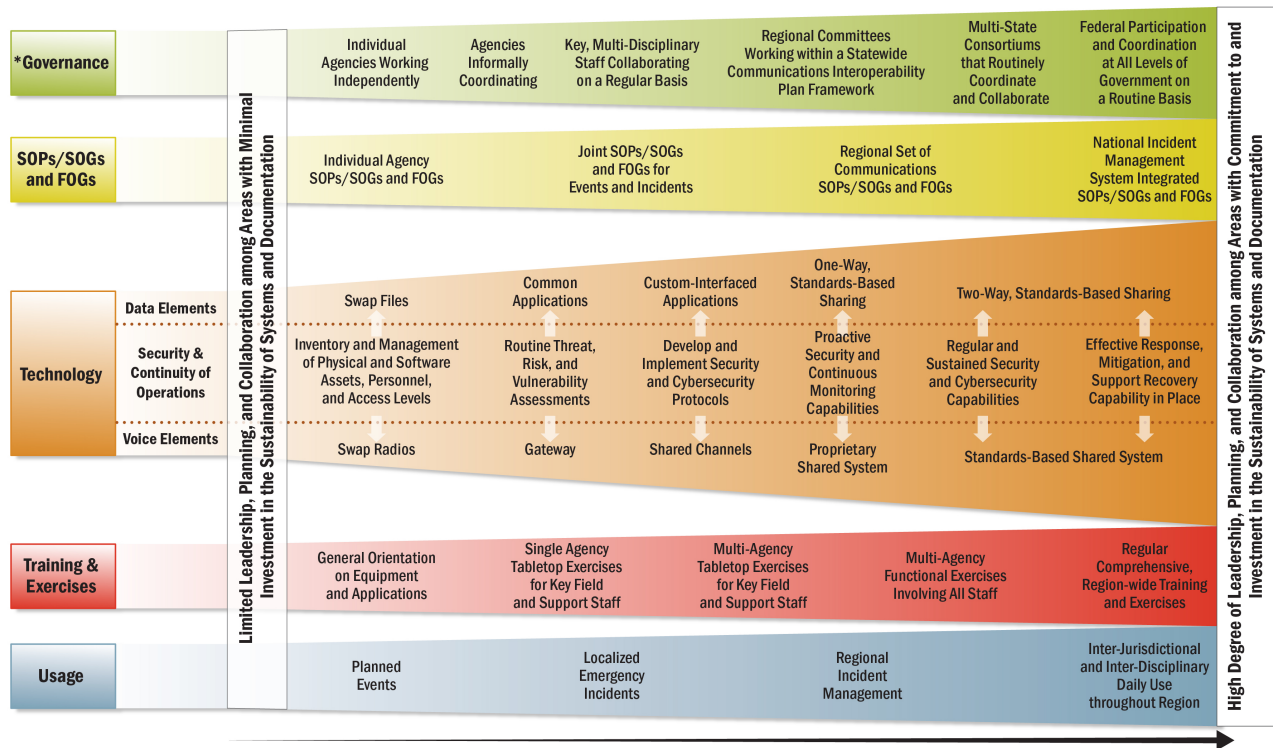
Figure 1: Interoperability Continuum

States can also structure their SCIP to align with the National Emergency Communications Plan (NECP), which provides guidance to drive enhancements of the Nation's emergency communications capabilities, through 6 overarching goals: Governance & Leadership; Planning & Procedures, Training, Exercise, & Evaluation; Communications Coordination; Technology & Infrastructure; and Cybersecurity. The Emergency Communications Ecosystem, depicted in the NECP, is comprised of the various functions and people that exchange information prior to, during, and after incidents. Key functions necessary to achieve reliable, secure, and interoperable emergency communications include Reporting and Requests for Assistance, Incident Coordination and Response, Alerts, Warnings, and Notifications, and Public Interaction.

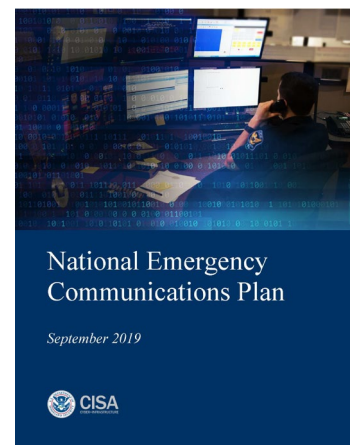*Figure 2: Emergency Communications Ecosystem*

Figure 3: National Emergency Communications Plan

CENTRAL FOCUS AREAS OF THE SCIP WORKSHOP

Feedback from states and territories over the last few years has led CISA to focus on the central areas of governance, technology, and funding sustainability as the framework for development of goals and objectives within the SCIP. However, states and territories may also choose to use one of the above-mentioned emergency communications frameworks (e.g., the Interoperability Continuum, the NECP and/or the State Interoperability Markers) instead to outline goals and objectives.

Governance

These workshops focus on enhancing statewide governance and public safety communications planning. In working with all 56 states and territories, CISA learned that states with the most effective governance typically have the highest levels of interoperability among the stakeholders. A strong governance structure allows for all lanes of the Interoperability Continuum to receive consideration and for implementation. The SCIP process will review in detail the state's current governance structure, to include capabilities and identified gaps. CISA facilitators will lead discussions on the key elements of effective governance to identify best practices that can be implemented in the state.

Cybersecurity

The cybersecurity security sections focus is on the continually evolving cyber risk landscape by reducing vulnerabilities and building resilience; countering malicious actors in cyberspace; responding to incidents; and making the cyber ecosystem more secure and resilient.

Technology

The technology section of the workshop focuses on technology's current state and ideal future state based on technological needs across all emergency communications technologies and capabilities. Stakeholders outline the SCIP to maintain and upgrade existing technology while developing a roadmap to identify and implement new and emerging technology solutions with a focus on the following:

Land Mobile Radio (LMR)

LMR has been the foundational public safety communications mechanism for half a century and is the primary lifeline of two-way, push-to-talk mission critical communications among public safety agencies. Participants discuss, plan, and develop goals critical to maintaining and modernizing LMR systems to ensure uninterrupted availability.

Broadband

Emerging broadband technologies promise to enhance all aspects of public safety communications. These technologies will augment the transport and sharing of voice, data, and video communications. Participants will discuss strategies for incorporating the broader use of broadband during day-to-day events and the planning for broadband data integration in large-scale public safety mutual-aid responses.

9-1-1

The use of 9-1-1 continues to be the public's lifeline to request help from public safety agencies; however, the migration from wired landline to cellular service has required operational changes within Public Safety Answering Points (PSAPS) and dispatch functions nationwide. Participants discuss the integration of modern technologies, strategies and associated challenges, and the transition from legacy 9-1-1 to Next Generation 9-1-1.

Alerts and Warnings

Another key system serving the public is the use of emergency alerting and warning systems. Examples of these systems would include Integrated Public Alerts & Warning System (IPAWS), National Weather Service alerts, reverse 9-1-1 and warning sirens. Participants may discuss and plan for how these systems will work in conjunction with other communications systems.

Funding Sustainability

SCIP workshop attendees also discuss strategies to fund existing and future interoperable and emergency communications priorities. States and territories seek to identify alternative sources of funding to maintain existing systems and capabilities, and to assist with the integration of new technologies to keep pace with the ever-changing emergency communications landscape.

SCIP PROCESS AND TIMELINE

Overview of the SCIP Process

Developing a strategic plan provides direction and focus for the entire state, including all agencies and jurisdictions, on the primary interoperable and emergency communications goals and initiatives. CISA's collaborative process gives agencies and jurisdictions an opportunity to be involved in shaping and defining statewide goals and initiatives to improve the likelihood of success for the development and implementation of a SCIP. To complete a SCIP, CISA developed a five-phased process for a recommended duration of eight to ten weeks to develop and conduct a workshop and deliver a completed SCIP to the Statewide Interoperability Coordinator (SWIC).

SCIP Planning Timeline

When a state or territory requests a SCIP workshop, there are a variety of planning milestones associated with ensuring the SWIC has all the materials, stakeholder commitments, and federal resources necessary to create a productive workshop. As an overall planning strategy, the desired course of action to provide an effective workshop is reflected in Figure 3 below.

Approximately eight to ten weeks prior to a desired on-site workshop, CISA and the SWIC will coordinate with stakeholders to develop the desired outcomes and participant list. During the planning process, the SWIC may utilize a survey to increase SCIP awareness, bring light to any new concerns, and gauge stakeholders' priorities related to emergency communications in their state. Following the pre-workshop planning process, CISA, in coordination with the SWIC, will develop all supporting materials necessary to ensure a successful meeting and an all-encompassing SCIP document. A draft SCIP will be delivered by CISA a few weeks following the workshop. Note, the planning process can be customized to meet the state's own completion date. The notional timeline below reflects the milestones and key steps in CISA's collaboration with states/territories in building a successful SCIP workshop and resulting plan.
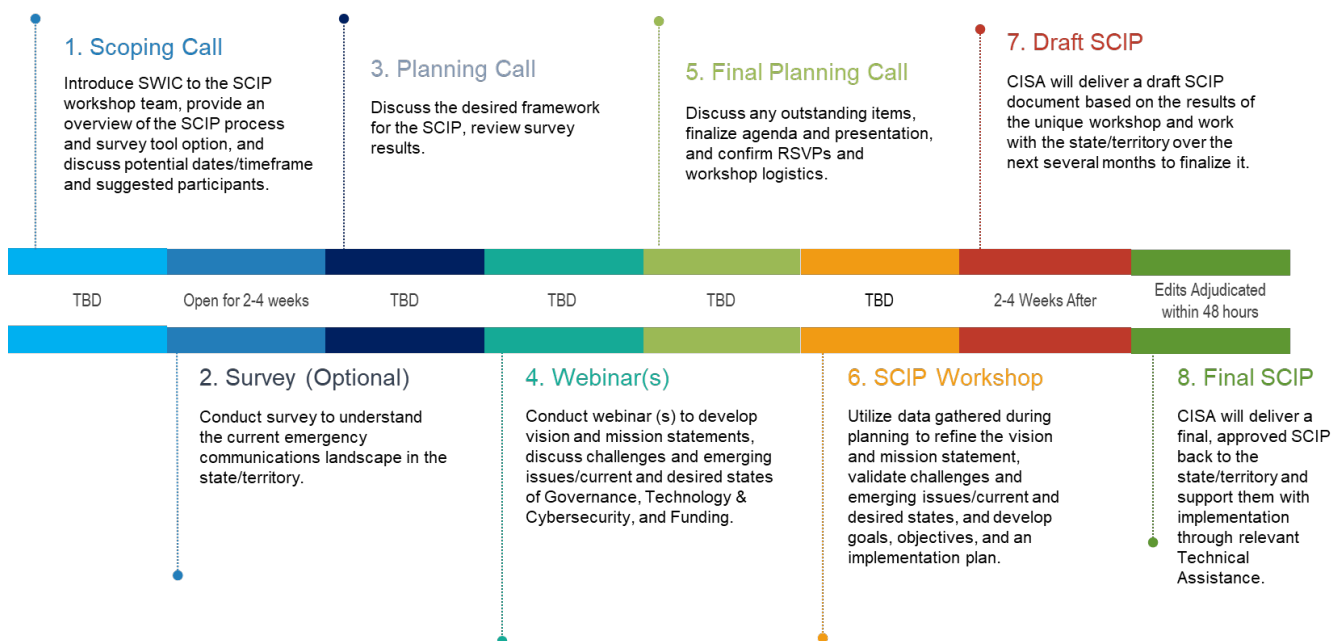

1. Scoping Call
Introduce SWIC to the SCIP workshop team, provide an overview of the SCIP process and survey tool option, and discuss potential dates/timeframe and suggested participants.

3. Planning Call
Discuss the desired framework for the SCIP, review survey results.

5. Final Planning Call
Discuss any outstanding items, finalize agenda and presentation, and confirm RSVPs and workshop logistics.

7. Draft SCIP
CISA will deliver a draft SCIP document based on the results of the unique workshop and work with the state/territory over the next several months to finalize it.

TBD | Open for 2-4 weeks | TBD | TBD | TBD | TBD | 2-4 Weeks After | Edits Adjudicated within 48 hours

2. Survey (Optional)
Conduct survey to understand the current emergency communications landscape in the state/territory.

4. Webinar(s)
Conduct webinar (s) to develop vision and mission statements, discuss challenges and emerging issues/current and desired states of Governance, Technology & Cybersecurity, and Funding.

6. SCIP Workshop
Utilize data gathered during planning to refine the vision and mission statement, validate challenges and emerging issues/current and desired states, and develop goals, objectives, and an implementation plan.

8. Final SCIP
CISA will deliver a final, approved SCIP back to the state/territory and support them with implementation through relevant Technical Assistance.

Figure 4: SCIP Process Timeline

WHO SHOULD ATTEND A SCIP WORKSHOP

The SCIP Workshop presents a unique opportunity to bring together a variety of stakeholders from across the state/territory for an intensive strategic planning workshop. When a diverse group collaborates to develop the SCIP, the result is a high-quality, executable plan with stakeholder ownership. Identifying key stakeholders that are relevant to the state/territory's interoperable and public safety communications efforts fosters strong working relationships while ensuring full representation in supporting the vision and mission of the SCIP. Subject matter experts and decision makers as well as representation from emerging technologies (broadband, NG 9-1-1, and alerts and warnings) should be included. During the planning phase, the SCIP team works with the SWIC to discuss the best approach to include leveraging CISA leadership and their sphere of influence to ensure broad attendance. CISA can also provide support with drafting invitation language that highlights state-specific information and create background materials for stakeholders to review prior to the workshop. CISA can disseminate workshop invitation and track RSVPs.

State Communications Leaders

- Statewide Interoperability Governing Body / Executive Committee
- Statewide Interoperability Coordinator
- Working Group Chairs
- FirstNet Single Point of Contact (SPOC)
- State Broadband Office / Committee Members
- 9-1-1 Board Members

State Government Leadership/Designee

- Executive and Legislative Leaders
- Governor's Office
- State Adjutant General
- Tribal Nation Representation
- Public Utility Commission
- Utility Regulation Authority
- Grants Coordinator
- State Chief Financial Officer
- State Chief Information Officer
- State Chief IT Security Officer
- State Chief Technology Officer
- Department of Emergency Management
- ESF-2 Coordinator
- State Director of Homeland Security
- State 9-1-1 Administrator Emergency Communications Office
- Incident Management Teams
- State EMAC Coordinator
- State Training Officer
- Regional Exercise Officer
- Public Safety Academy/Dispatch Training

Public Safety/Public Service Entities

- FirstNet Regional Representatives
- 9-1-1/PSAP Officials
- Corrections
- Emergency Management
- Emergency Medical Services
- Fire Departments
- Law Enforcement
- Public Health
- Public Safety Communications Network Operators
- Public Works
- Department of Transportation
- Department of Health
- Maritime/Port Authorities
- State or Regional Fusion centers
- Other Federal partners

Associations

- Association of Chiefs of Police
- State Sheriff's Association
- National Emergency Number Association
- National Association of State 9-1-1 Administrators
- National Association of CIOs
- Association of Counties
- Association of EMS Administrators
- Association of Public-Safety Communications Officials
- Emergency Management Associations
- Fire Chiefs' Association
- State Fire Fighters' Associations
- Hospital and Public Health Associations
- Public Works Associations
- Other associations of elected leaders (County Commissioners, Judges, etc.)
- State-level Amateur Radio Organizations

Other Entities

- Board of Regents
- College and University Public Safety
- Bordering State SWICs
- Communications Industry
- Rail Industry
- Non-Governmental Organizations
- Regional Councils of Government
- Municipal Government Leadership
- Private Public Safety Entities
- Underrepresented communities
- Critical Infrastructure partners

SWIC CHECKLIST

Scoping Call

- ☐ Discuss desired planning framework/approach
  - o Most states follow the three-webinar approach, having a webinar for: Governance, Technology and Cybersecurity, and Funding
  - o While it is highly encouraged to conduct an In-Person SCIP workshop, the workshop can be delivered virtually or in a hybrid format to encourage as many participants as possible
- ☐ Engage SWIC on use of State Survey
- ☐ Discuss variety of services CISA can provide throughout process
- ☐ Identify timeline and workshop logistics

Survey Design

- ☐ Provide feedback on templated survey questions and customize it to meet state-specific outcomes
- ☐ Discuss suggested participants
- ☐ Disseminate the survey

Planning Call

- ☐ Provide feedback on templated survey questions and customize it to meet state-specific outcomes
- ☐ Discuss suggested participants
- ☐ Disseminate the survey

Webinar(s)

- ☐ Review Planning Call Summary and provide any feedback
- ☐ Review live capture document with current and desired state / successes, challenges, and emerging issues and provide any feedback
- ☐ Invite suggested participants to SCIP workshop

Final Planning Call

- ☐ Provide any final edits to the workshop agenda, updated list of RSVPs, and any outstanding items
- ☐ Confirm workshop location and logistics (schedule walkthrough of venue if in-person)

SCIP Workshop

- ☐ Review workshop logistics
- ☐ Review live capture document with goals, objectives, and an implementation and provide any feedback
- ☐ Hotwash with internal team and SWIC