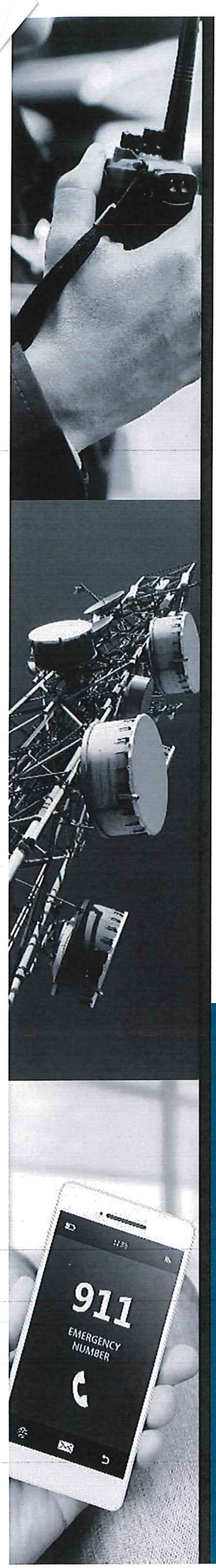


CONNECTICUT
STATEWIDE COMMUNICATION INTEROPERABILITY PLAN

October 2022

Developed by the Connecticut Public Safety Interoperable Communications Executive Committee with Support from the Cybersecurity and Infrastructure Security Agency

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LETTER FROM THE STATEWIDE INTEROPERABILITY COORDINATOR AND THE STATE EMERGENCY MANAGEMENT DIRECTOR

Greetings,

As the Statewide Interoperability Coordinator (SWIC) for Connecticut, and the State Emergency Management Director, we are pleased to present to you the 2022 Connecticut Statewide Communication Interoperability Plan (SCIP). The SCIP represents the State's continued commitment to improving emergency communications interoperability and supporting the public safety practitioners throughout the State. In addition, this update meets the requirement of the current U.S. Department of Homeland Security grant guidelines.

Representatives from the Connecticut Public Safety Interoperable Communications Executive Committee (CPSICEC) collaborated with Connecticut public safety officials to update the SCIP with actionable and measurable goals and objectives that have champions identified to ensure completion. These goals and objectives focus on Governance, Technology and Cybersecurity, and Funding. They are designed to support our State in planning for emerging technologies and navigating the ever-changing emergency communications landscape. They also incorporate the SAFECOM/National Council of SWICs (NCSWIC) State Interoperability Markers which describe Connecticut's level of interoperability maturity by measuring progress against 25 markers.

As we continue to enhance interoperability, we must remain dedicated to improving our ability to communicate among disciplines and across jurisdictional boundaries. With help from public safety practitioners statewide, we will work to achieve the goals set forth in the SCIP and become a nationwide model for statewide interoperability.

Sincerely,

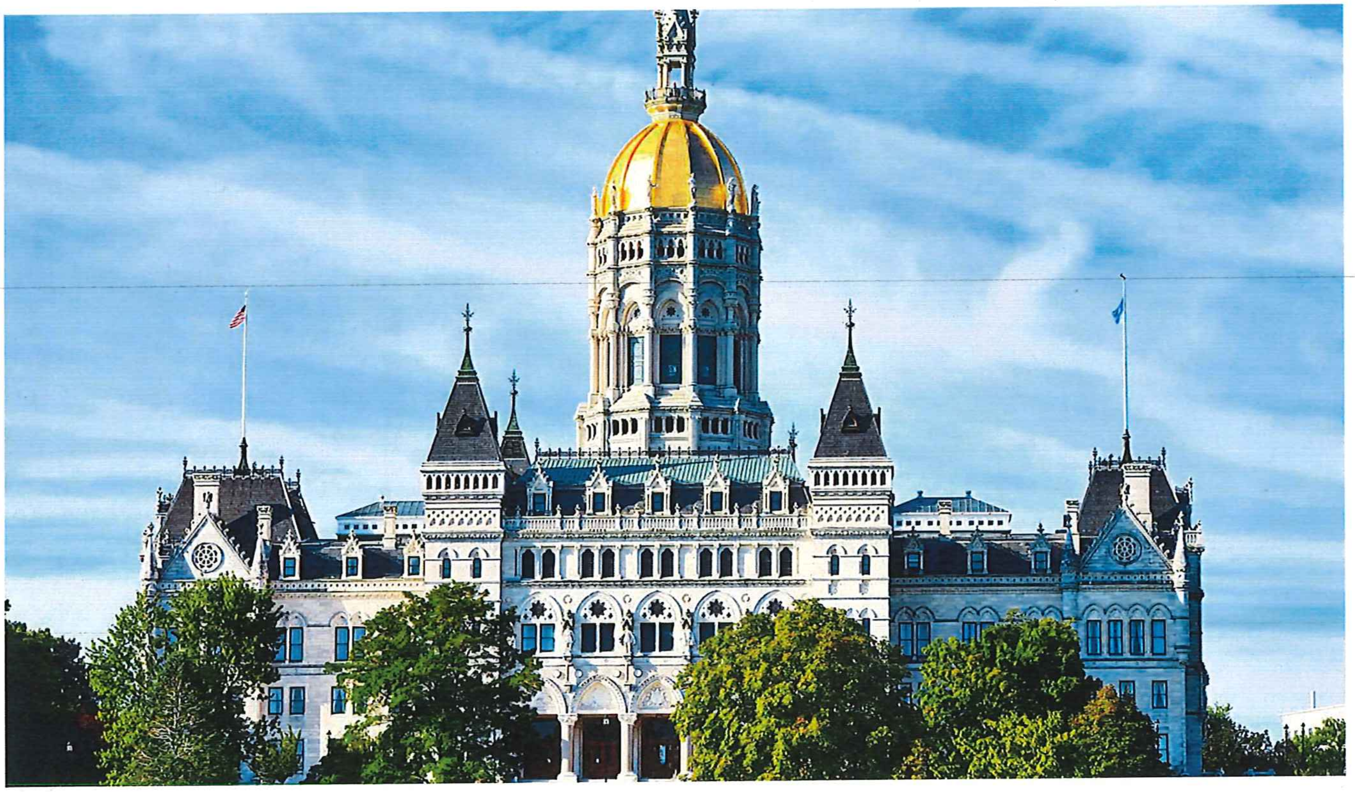
Clayton Northgraves

Clayton Northgraves, ENP
Director of Statewide Emergency Telecommunications,
Connecticut Statewide Interoperability Coordinator (SWIC), Co-Chair SIEC
Connecticut Department of Emergency Services and Public Protection

William H. Turner

William H. Turner
State Emergency Management Director, Co-Chair SIEC
Division of Emergency Management and Homeland Security
Connecticut Department of Emergency Services and Public Protection

INTRODUCTION



The SCIP is a one-to-three-year strategic planning document that contains the following components:

- **Introduction** – Provides the context necessary to understand what the SCIP is and how it was developed. It also provides an overview of the current emergency communications landscape.
- **Vision and Mission** – Articulates Connecticut's vision and mission for improving emergency and public safety communications interoperability over the next one-to-three-years.
- **Governance** – Describes the current governance mechanisms for communications interoperability within Connecticut as well as successes, challenges, and priorities for improving it. The SCIP is a guiding document and does not create any authority or direction over any state or local systems or agencies.
- **Technology and Cybersecurity** – Outlines public safety technology and operations needed to maintain and enhance interoperability across the emergency communications ecosystem.
- **Funding** – Describes the funding sources and allocations that support interoperable communications capabilities within Connecticut along with methods and strategies for funding sustainment and enhancement to meet long-term goals.
- **Tribal** – Provides an overview of Connecticut's tribal interoperable communications and relationship within the state.

- **Implementation Plan** – Describes Connecticut's plan to implement, maintain, and update the SCIP to enable continued evolution of and progress toward the State's interoperability goals.

The Emergency Communications Ecosystem consists of many inter-related components and functions, including communications for incident response operations, notifications, alerts, and warnings, requests for assistance and reporting, and public information exchange. The primary functions are depicted in the 2019 National Emergency Communications Plan.[1]

The Interoperability Continuum, developed by the Department of Homeland Security's SAFECOM program and shown in Figure 1, serves as a framework to address challenges and continue improving operable/interoperable and public safety communications.[2] It is designed to assist public safety agencies and policy makers with planning and implementing interoperability solutions for communications across technologies.

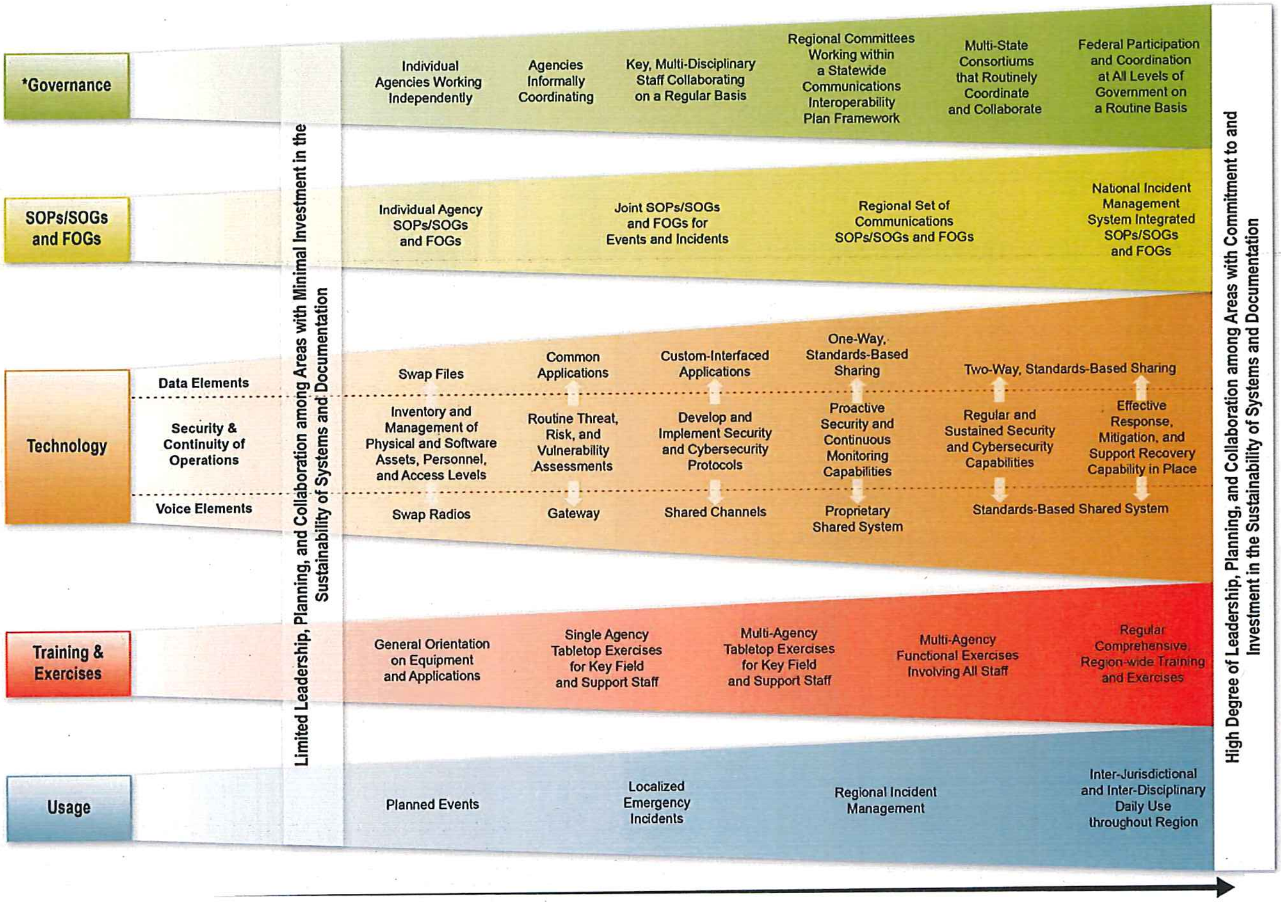

*Governance
Individual Agencies Working Independently
Agencies Informally Coordinating
Key, Multi-Disciplinary Staff Collaborating on a Regular Basis
Regional Committees Working within a Statewide Communications Interoperability Plan Framework
Multi-State Consortiums that Routinely Coordinate and Collaborate
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
Security & Continuity of Operations
Voice Elements
Swap Files
Common Applications
Custom-Interfaced Applications
One-Way, Standards-Based Sharing
Two-Way, Standards-Based Sharing
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
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
Limited Leadership, Planning, and Collaboration among Areas with Minimal Investment in the Sustainability of Systems and Documentation
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

Interoperability and Emergency Communications Overview

Interoperability is the ability of emergency response providers and relevant government officials to communicate across jurisdictions, disciplines, and levels of government as needed and as

[1] 2019 National Emergency Communications Plan

[2] Interoperability Continuum Brochure

authorized. Reliable, timely communications among public safety responders and between public safety agencies and citizens is critical to effectively carry out public safety missions, and in many cases, saving lives.

Traditional voice capabilities, such as land mobile radio (LMR) and landline 9-1-1 services have long been and continue to be critical tools for communications. However, the advancement of internet protocol-based technologies in public safety has increased the type and amount of information responders receive, the tools they communicate with, and complexity of new and interdependent systems. Emerging technologies increase the need for coordination across public safety disciplines, communications functions, and levels of government to ensure emergency communications capabilities are interoperable, reliable, and secure.

An example of this evolution is the transition of public-safety answering points (PSAPs) to Next Generation 9-1-1 (NG9-1-1) technology that will enhance sharing of critical information in real-time using multimedia—such as pictures, video, and text — among citizens, PSAP operators, dispatch, and first responders. While potential benefits of NG9-1-1 are tremendous, implementation challenges remain. Necessary tasks to fully realize these benefits include interfacing disparate systems, developing training and standard operating procedures (SOPs) and ensuring information security.

VISION AND MISSION

This section describes Connecticut's vision and mission for improving emergency and public safety communications interoperability, emphasizing operationally appropriate compatible systems and data platforms, (e.g., federal, state, regional, local, tribal nations, private sector, and non-government organizations).

Vision:

Provide and sustain a common interoperable communications pathway for all involved stakeholders

Mission:

Continue to enhance and sustain a standards-based communications infrastructure that will allow for secure, timely, efficient, flexible, and cost-effective statewide and regional interoperability

GOVERNANCE

The Connecticut SIEC is called the Connecticut Public Safety Interoperable Communications Executive Committee (CPSICEC) a subcommittee of the DEMHS Advisory Council as established by the Deputy Commissioner of DESPP responsible for the Division of Emergency Management and Homeland Security (DEMHS). The SIEC is organized under Title 28 of the Connecticut General Statutes and meets quarterly to coordinate interoperability issues within the state. See Sections

28-1a(b) and 29-1b(b). The CSPICEC is comprised of state and local fire, police, medical, transportation, IT, emergency management personnel and tribal representation. The SIEC's primary purpose is to provide recommendations to the Deputy Commissioner of DEMHS and to the Advisory Council about sharing real-time voice, video, and data information with authorized first responders and other critical components of the emergency management and public safety community. Connecticut's SWIC position has recently moved from the Division of Emergency Management and Homeland Security (DEMHS) to Division of Statewide Emergency Telecommunications (DSET). There are two federally recognized Native American Tribes in Connecticut the Mashantucket Pequot and Mohegan tribes along with 5 state recognized tribes.

It should be noted that Connecticut currently has regional Tactical Interoperability Communication Plan's (TICP).

Connecticut's governance structure is depicted in Figure 2.

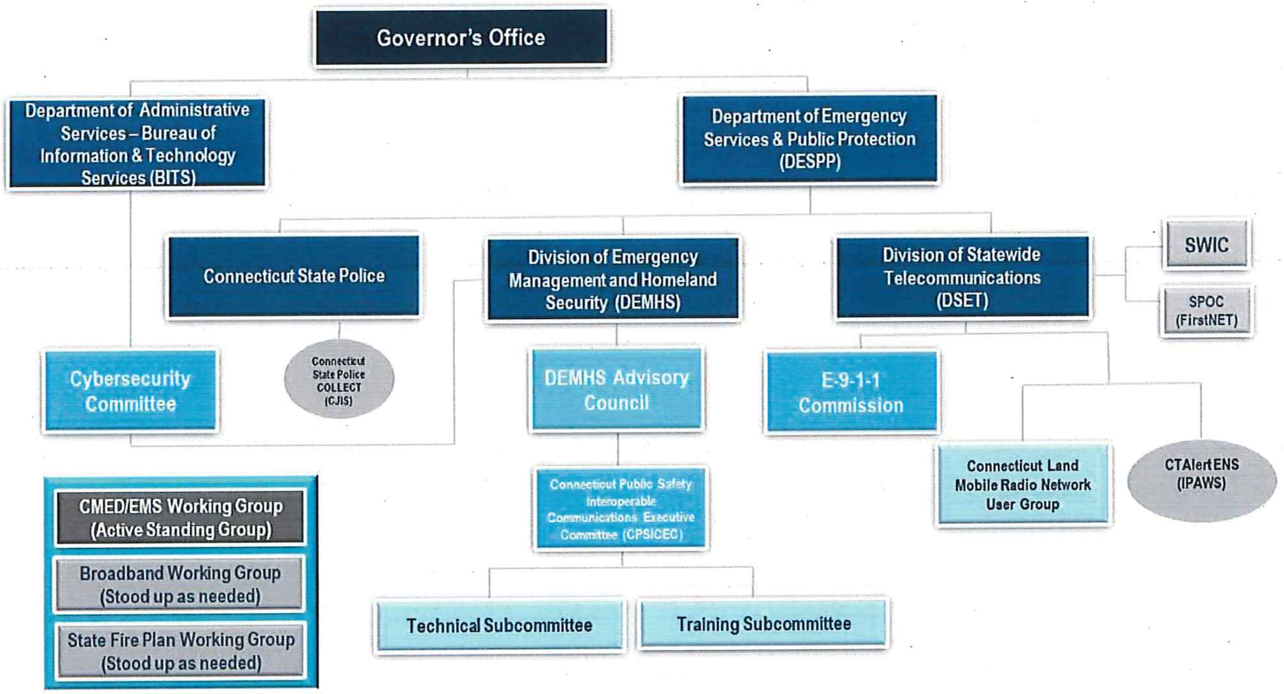

Governor's Office
Department of Administrative Services – Bureau of Information & Technology Services (BITS)
Department of Emergency Services & Public Protection (DESPP)
Connecticut State Police
Division of Emergency Management and Homeland Security (DEMHS)
Division of Statewide Telecommunications (DSET)
SWIC
SPOC (FirstNET)
Cybersecurity Committee
Connecticut State Police COLLECT (CJIS)
DEMHS Advisory Council
E-9-1-1 Commission
Connecticut Land Mobile Radio Network User Group
CTAlert ENS (IPAWS)
CMED/EMS Working Group (Active Standing Group)
Broadband Working Group (Stood up as needed)
State Fire Plan Working Group (Stood up as needed)
Connecticut Public Safety Interoperable Communications Executive Committee (CPSICEC)
Technical Subcommittee
Training Subcommittee

Figure 2: Connecticut's Governance Structure

The following table outlines goals and objectives related to Governance:

Governance	
Goal	**Objectives**
1. Update and enhance inter-and intra-state regional coordination on operable and interoperable communications activities and efforts	1.1 Update SIEC listserv to ensure RESF 2 committees are included in the distribution of meeting minutes
	1.2 Amend SIEC Bylaws to ensure all regions have alternative voting member representation at SIEC meetings
	1.3 Maintain communications with FEMA Regions I and II and their respective States

Goal	Objectives
2. Continue presence on national committees (e.g., Public Safety Advisory Committee [PSAC], Northeast States Emergency Consortium [NESEC], Regional Emergency Communications Coordination Working Groups [RECCWGs], National Emergency Management Association [NEMA], National Council of Statewide Interoperability Coordinators [NCSWIC], SAFECOM)	2.1 Identify target national committees on which to participate for communications issues
	2.2 Identify personnel to participate on national committees for communications issues
	2.3 Communicate information from national committees to the regions for communications issues
3. Build on established SOPs to include non-traditional public safety response partners (e.g., utilities, NGOs) in the initial notification of an incident or event	3.1 Revise State and regional lists of non-traditional public safety response partners or secondary end-users to include in pre-notification (e.g., utilities, NGOs)
	3.2 Continue to develop relationships with identified non-traditional public safety response partners (e.g., utilities, NGOs)
	3.3 Identify pre-notification methods (e.g., list serves)
	3.4 Establish a mentoring program to identify and develop the next generation of expertise
4. Create interoperable communications and broadband SOPs that are regularly updated and stored in a centralized repository that enables sharing across regions and municipalities	4.1 Identify existing interoperable communications and broadband SOPs and conduct a gap analysis
	4.2 Develop new SOPs based on identified gaps and by grant guidance
	4.3 Identify pre-notification methods (e.g., list serves)
	4.4 Review SOPs for State and National Response Frameworks (SRF/NRF) and National Incident Management System (NIMS) compliance and update as needed
	4.5 Establish a mentoring program to identify and develop the next generation of expertise
5. Document and coordinate use of best practices for redundancy/resiliency of existing Public Safety Answering Points (PSAP)	5.1 Develop an emergency communications architecture best practices document for PSAPs, leveraging national standards
6. Complete cyber risk and security assessments for existing systems and make appropriate improvements	6.1 Develop best practices guide for minimum cybersecurity protection
	6.2 Identify the existing systems requiring cyber risk and security assessments
	6.3 Establish a plan to complete assessments based on funding availability
	6.4 Identify additional funding as needed
7. Identify and enhance the integration and use of data	7.1 Identify existing data systems and data format compatibility among those systems

Goal	Objectives
sharing and standard operating systems (e.g., WebEOC, LPR, disaster recovery software) used for emergency and disaster response	7.2 Standardize data reporting format
8. Promote the use of specific communications components/resources (e.g., COMU personnel, STR/interoperable equipment, communications objectives/injects) into trainings, exercises, planned and real-world events, where appropriate	8.1 Identify training and exercise opportunities, including those on the statewide multi-year training and exercise calendar, to leverage existing opportunities to integrate communications components/resources
	8.2 Through outreach, promote the use and capabilities of specialized and trained COMU personnel and STR/interoperability equipment at trainings, exercises, planned and real-world events
9. Provide end-user training for more effective and efficient interoperable communications	9.1 Develop standardized end user training for operable and interoperable communications for basic level responders, mid-level supervisors and executive leadership, to include classroom trainings, online trainings, field training guides, etc.
	9.2 Develop a deployment plan for the standardized trainings to reach the intended first responder audience
	9.3 Identify professional associations and other training organizations that currently provide training to first responders in the state (academies, etc.), to promote incorporating the updated training on communications fundamentals into their curriculum
	9.4 Provide the standardized end user training to the existing associations and organizations identified in 9.4
10. Reinvigorate/formalize the Connecticut COMU	10.1 Develop a COMU plan to include: operational and deployment SOPs; training, certification, and re-certification requirements; tracking system for COMU position candidates and members; and best practices for use of COMU personnel to ensure maximization of resources.
	10.2 Promote the use and capabilities of specialized and trained COMU personnel through outreach
	10.3 Identify additional trainings and exercises needed for COMU personnel
11. Maintain a schedule for the systematic, monitoring and/or testing and use of interoperable systems, STR/cache equipment, and channels or talk groups	11.1 Identify resources that require testing and frequency of testing
	11.2 Develop and publish a monitoring/testing schedule and align with existing testing, as applicable

TECHNOLOGY AND CYBERSECURITY

Land Mobile Radio

The Connecticut Land Mobile Radio Network (CLMRN) is a Statewide P25 7/800 MHz Trunked/Simulcast system. The Division of Statewide Emergency Telecommunications (DSET) oversees the Connecticut Land Mobile Radio Network (CLMRN). The Connecticut Land Mobile Radio Network Unit (CLMRN) is comprised of several subsystems that are integrated into a statewide communications network. There is currently 98% mobile coverage throughout the State. Connecticut has an 8CALL/8TAC interoperability mutual aid radio system, along with a State tactical on scene channel system (STOCS) which is a combined UHF/VHF/800 MHz interoperability channel group. There are multiple bi-directional amplifiers (BDA) and distributed antenna (DAS) systems utilized to enhance voice and data interoperability. Connecticut tribes have their own LMR systems with gateway technology that links tribal systems to the state system. The State of Connecticut Emergency Services (EMS) communicates with hospitals using the Centralized Medical Emergency Direction system (CMED). These CMED's track times, provide ambulance to hospital radio patches, telemetry information, multiple casualty incident MCI, and mutual aid coordination. There 12 total CMEDs. There is currently approximately 50% of the state integrated on the CLMRN.

9-1-1/Next Generation 9-1-1

The Division of Statewide Telecommunications (DSET) is responsible for statewide Enhanced 9-1-1 (E9-1-1) planning, equipment, and implementation, including NG9-1-1 services. DSET recently replaced E9-1-1 with NG9-1-1. NG9-1-1 is fully integrated with the statewide system. Connecticut currently has 106 primary public safety answering points (PSAPs) and averaging over 1.9 million calls per year. There are two tribal PSAPs.

Broadband

Connecticut currently uses a Public Safety Data Network (PSDN) which is an ultra-high-speed fiber optic data network for approximately 400 public safety government applications and services statewide. Connecticut chose to opt in the FirstNet plan. The state along with the tribes are engaged with FirstNET to discuss public safety broadband needs. The state plans to obtain 6 Compact Rapid Deployables (CRDs) which are standalone cellular towers which provide cellular and internet connectivity for use during network outages or in areas where cellular service is unavailable or unreliable, with Band 14 cellular coverage, Wi-Fi capability, and an integrated Ka-Band satellite system. There are currently 3 carriers providing services in the state, those carries are ATT/FirstNet, Verizon, and T-Mobile.

Alerts and Warnings

The State of Connecticut has implemented a state-of-the-art emergency notification system to alert residents about emergencies. The CTAlert - Emergency notification system, enables state and local 911 emergency communication centers to provide essential information quickly in a variety of emergency situations and is managed by DSEPP through DSET. CTAlert is powered by Everbridge Mass Notifications a global provider of software as a service (SaaS)-based unified critical communications. Everbridge, enables Connecticut authorities to communicate critical information directly to every hospital, emergency response agency, business, and resident across the state to keep them safe and informed. The system is used for both emergencies and important day-to-day operations. There are currently 6 PSAPs statewide that have elected not to have CTAlert. Connecticut also has an Integrated Public Alerts and Warning System (IPAWS) which is managed by the State. The Tribes utilizes the State's Everbridge Alerting system and operate a sperate tribal only alerting system.

National Warning System (NAWAS) - NAWAS is a voice communications system operated by the Federal Emergency Management Agency (FEMA) under the U.S. Department of Homeland Security (DHS) and controlled from the FEMA Operations Center (FOC) in Washington, DC, and the FEMA Alternate Operations Center (FAOC) in Olney, Maryland. NAWAS is a 24-hour nationwide, dedicated, multiple line telephone warning system linking federal agencies and the states, and is used to disseminate civil emergency warnings. CT-DESPP/DEMHS serves as the Alerting Authority for this system with the DESPP Message Center acting as State Warning Point for the NAWAS and guards both State and Federal terminals for alert dissemination.

Emergency Alert System (EAS) - CT-DESPP/DEMHS, as the State Alerting Authority, is responsible for Connecticut's use of the Federally mandated Emergency Alerting System (EAS). Activation of the EAS system can take place from either the DESPP Message Center or State EOC. The purpose of the EAS is to provide real-time communication, information, direction, and instruction in the event of an emergency requiring public action and may be activated at the federal, state, or local level. The EAS utilizes commercial radio and television broadcast services, which are provided on a voluntary, organized basis. CT-DESPP/DEMHS is certified through the IPAWS program. Use of the EAS System is outlined in the Connecticut EAS Plan.

Cybersecurity

The State of CT has a strategic State of CT Cybersecurity Strategy (last approved March 2022), which sets forth seven foundational principles including executive leadership, awareness, literacy, preparation, response, recovery, communication and verification. This document is intended to lead the way in cybersecurity planning in Connecticut.

The Bureau of Indian Affairs (BIA) provides cybersecurity resources to the tribes.

FUNDING

The Department of Emergency Services and Public Protection (DESPP) serves as the State Administrative Agent (SAA) through DEMHS and is the State's eligible applicant for programmatic administer of the Emergency Management Performance Grant (EMPG) and Homeland Security Grant (HSGP) funds. Communications projects are funded using a variety of sources: HSGP to the five DEMHS Regions, EMPG for local and State projects, and State General and Bond Funds.

DEMHS makes an EMPG Workplan every year that shows how EMPG funds will be used to meet both short-term and long-term goals. The state gives local governments a certain amount of the total federal money that can be used for eligible costs. Through a matching reimbursement program, the EMPG State and Local Assistance (SLA) program gives money to communities for eligible personnel, training, equipment, and operating costs related to their emergency management program. DEMHS also provides matched EMPG funding (no town match required) for all local communications projects.

The Regional Collaboration Committee gives the opportunity for all grant stakeholders to meet and agree upon the use of yearly allocated HSGP program funding. Applications for HSGP funding are influenced by the recommendations set forth by this committee and is a requirement the Federal Homeland Security Grant Program.

It should be noted that the tribes utilize a five-year life cycle replacement plan for technology.

Funding goals and objectives include the following:

Funding	
Goal	**Objectives**
12. Sustainment funding for maintenance of interoperable communications in the state	12.1 Identify the life cycle and funding requirements of significant systems and equipment to demonstrate long-term budget requirements to financial decision-makers
	12.2 Leverage stakeholder groups (e.g., professional associations) to present the business case for sustaining interoperable and emergency communications systems to legislators

TRIBAL

As mentioned above, there are two federally recognized Native American Tribes in Connecticut, the Mashantucket Pequot and Mohegan tribes. The state recognizes five additional tribes. A member of the Mohegan tribe serves on the CSPICEC as the state's tribal representative. Each of the federally recognized tribes have their own public safety agencies, PSAPs along with designated Emergency Management Directors.

Governance – Tribal representatives noted the importance of interoperability with other Connecticut first responders and have a representative on the CSPICEC. MOUs currently exist to share capabilities and services. The tribes are conscious of the need for interoperability with their partners and there is a desire to be an example to others regarding interoperable communications and collaboration.

Technology – Both the Mashantucket Pequot and Mohegan tribes have land mobile radio systems, and the capabilities exist for connectivity with the state. The tribes are conscious of the need for alerts and warnings and currently use the Everbridge system. Broadband capabilities exist with the tribes, and they are engaged with FirstNet. Physical separation of public safety systems and the elimination of single points of failure have been a priority for public safety technology systems.

Cybersecurity – Beyond physical separation of public safety system components the tribes work closely with the Bureau of Indian Affairs (BIA) for cybersecurity and resiliency. It was noted that there is 1000+ attempts at cyber breaches per day.

Funding – The tribes employ best practices for funding utilizing a 5-year lifecycle management plan and 3-year plan for new technologies. The tribes work with BIA and have their own grant administrator.

IMPLEMENTATION PLAN

Each goal and its associated objectives have a timeline with a target completion date, and one or multiple owners that will be responsible for overseeing and coordinating its completion. Accomplishing goals and objectives will require the support and cooperation from numerous individuals, groups, or agencies, and will be added as formal agenda items for review during regular governance body meetings. The Cybersecurity and Infrastructure Security Agency's (CISA) Interoperable Communications Technical Assistance Program (ICTAP) has a catalog[3] of technical assistance (TA) available to assist with the implementation of the SCIP. TA requests are to be coordinated through the SWIC.

Based on the discussions during the SCIP Workshop, CISA recommends the following TAs to support Connecticut's SCIP goals:

- Grant Funding for Emergency Communications Webinar
- Governance Documentation Review and Development (GOV-DOC)
- Communications Unit Leader (COML)
- Communications Unit Planning and Policies (COMUPLAN)

Connecticut's implementation plan is shown in the table below.

Goals	Objectives	Owners	Completion Date
1. Update and enhance inter-and intra-state regional coordination on operable and interoperable communications activities and efforts	1.1 Update SIEC listserv to ensure RESF 2 committees are included in the distribution of meeting minutes	DEMHS SWIC	April 2023
	1.2 Amend SIEC Bylaws to ensure all regions have alternative voting member representation at SIEC meetings		
	1.3 Maintain communications with FEMA Regions I and II and their respective States		
2. Continue presence on national committees (e.g., Public Safety Advisory Committee [PSAC], Northeast States Emergency	2.1 Identify target national committees on which to participate for communications issues	SWIC DEMHS	Ongoing
	2.2 Identify personnel to participate on national committees for communications issues		

[3] Emergency Communications Technical Assistance Planning Guide

Goals	Objectives	Owners	Completion Date
Consortium [NESEC], Regional Emergency Communications Coordination Working Groups [RECCWGs], National Emergency Management Association [NEMA], National Council of Statewide Interoperability Coordinators [NCSWIC], SAFECOM)	2.3 Communicate information from national committees to the regions for communications issues		
3. Build on established SOPs to include non-traditional public safety response partners (e.g., utilities, NGOs) in the initial notification of an incident or event	3.1 Revise State and regional lists of non-traditional public safety response partners or secondary end-users to include in pre-notification (e.g., utilities, NGOs)	SIEC	Ongoing 3.4 – October 2023
	3.2 Continue to develop relationships with identified non-traditional public safety response partners (e.g., utilities, NGOs)		
	3.3 Identify pre-notification methods (e.g., list serves)		
	3.4 Establish a mentoring program to identify and develop the next generation of expertise		
4. Create interoperable communications and broadband SOPs that are regularly updated and stored in a centralized repository that enables sharing across regions and municipalities	4.1 Identify existing interoperable communications and broadband SOPs and conduct a gap analysis	SIEC	Ongoing 4.5 – October 2023
	4.2 Develop new SOPs based on identified gaps and by grant guidance		
	4.3 Identify pre-notification methods (e.g., list serves)		
	4.4 Review SOPs for State and National Response Frameworks (SRF/NRF) and National Incident Management System (NIMS) compliance and update as needed		
	4.5 Establish a mentoring program to identify and develop the next generation of expertise		
5. Document and coordinate use of best practices for redundancy/resiliency of existing Public Safety Answering Points (PSAP)	5.1 Develop an emergency communications architecture best practices document for PSAPs, leveraging national standards	DSET 911 Commission	October 2024
	6.1 Develop best practices guide for minimum cybersecurity protection	DEMHS	6.1 – April 2023

Goals	Objectives	Owners	Completion Date
6. Complete cyber risk and security assessments for existing systems and make appropriate improvements	6.2 Identify the existing systems requiring cyber risk and security assessments	Cybersecurity Committee BITS	6.2 – October 2023 6.3 – October 2023 and ongoing 6.4 - Ongoing
	6.3 Establish a plan to complete assessments based on funding availability		
	6.4 Identify additional funding as needed		
7. Identify and enhance the integration and use of data sharing and standard operating systems (e.g., WebEOC, LPR, disaster recovery software) used for emergency and disaster response	7.1 Identify existing data systems and data format compatibility among those systems	SIEC DEMHS DSET	October 2025
	7.2 Standardize data reporting format		
8. Promote the use of specific communications components/resources (e.g., COMU personnel, STR/interoperable equipment, communications objectives/injects) into trainings, exercises, planned and real-world events, where appropriate.	8.1 Identify training and exercise opportunities, including those on the statewide multi-year training and exercise calendar, to leverage existing opportunities to integrate communications components/resources	DEMHS SIEC	Ongoing
	8.2 Through outreach, promote the use and capabilities of specialized and trained COMU personnel and STR/interoperability equipment at trainings, exercises, planned and real-world events		
9. Provide end-user training for more effective and efficient interoperable communications	9.1 Develop standardized end user training for operable and interoperable communications for basic level responders, mid-level supervisors and executive leadership, to include classroom trainings, online trainings, field training guides, etc.	DEMHS SIEC	9.1 - October 2023 9.2 - October 2023 9.3 - October 2023 9.4 - October 2023 Ongoing
	9.2 Develop a deployment plan for the standardized trainings to reach the intended first responder audience		
	9.3 Identify professional associations and other training organizations that currently provide training to first responders in the state (academies, etc.), to promote incorporating the updated training on communications fundamentals into their curriculum		
	9.4 Provide the standardized end user training to the existing associations and organizations identified in 9.4		

Goals	Objectives	Owners	Completion Date
10. Reinvigorate/formalize the Connecticut COMU	10.1 Develop a COMU plan to include: operational and deployment SOPs; training, certification, and re-certification requirements; tracking system for COMU position candidates and members; and best practices for use of COMU personnel to ensure maximization of resources.	SIEC	October 2023, Ongoing
	10.2 Promote the use and capabilities of specialized and trained COMU personnel through outreach		
	10.3 Identify additional trainings and exercises needed for COMU personnel		
11. Maintain a schedule for the systematic Monitoring and /or testing and use of interoperable systems, STR/cache equipment, and channels or talk groups	11.1 Identify resources that require testing and frequency of testing	System and resource custodial owners DEMHS SIEC DSET	April 2023, Ongoing
	11.2 Develop and publish a monitoring/testing schedule and align with existing testing, as applicable		
12. Sustainment funding for maintenance of interoperable communications in the state	12.1 Identify the life cycle and funding requirements of significant systems and equipment to demonstrate long-term budget requirements to financial decision-makers	Custodial owners DEMHS DSET REPT (Regional Emergency Planning Teams)	Annual
	12.2 Leverage stakeholder groups (e.g., professional associations) to present the business case for sustaining interoperable and emergency communications systems to legislators		

APPENDIX A: STATE MARKERS

In 2019, CISA supported States and Territories in establishing an initial picture of interoperability nationwide by measuring progress against 25 markers. These markers describe a State or Territory's level of interoperability maturity. Below is [STATE/TERRITORY'S] assessment of their progress against the markers.

Marker	Best Practices / Performance Markers	Initial	Defined	Optimized
1	**State-level governing body established (e.g., SIEC, SIGB).** Governance framework is in place to sustain all emergency communications	Governing body does not exist, or exists and role has not been formalized by legislative or executive actions	Governing body role established through an executive order	Governing body role established through a state law
2	**SIGB/SIEC participation.** Statewide governance body is comprised of members who represent all components of the emergency communications ecosystem.	Initial (1-2) Governance body participation includes: ☐ Communications Champion/SWIC ☐ LMR ☐ Broadband/LTE ☐ 9-1-1 ☐ Alerts, Warnings and Notifications	Defined (3-4) Governance body participation includes: ☐ Communications Champion/SWIC ☐ LMR ☐ Broadband/LTE ☐ 9-1-1 ☐ Alerts, Warnings and Notifications	Optimized (5) Governance body participation includes: ☒ Communications Champion/SWIC ☒ LMR ☒ Broadband/LTE ☒ 9-1-1 ☒ Alerts, Warnings and Notifications
3	**SWIC established.** Full-time SWIC is in place to promote broad and sustained participation in emergency communications.	SWIC does not exist	Full-time SWIC with collateral duties	Full-time SWIC established through executive order or state law
4	**SWIC Duty Percentage.** SWIC spends 100% of time on SWIC-focused job duties	SWIC spends >1, <50% of time on SWIC-focused job duties	SWIC spends >50, <90% of time on SWIC-focused job duties	SWIC spends >90% of time on SWIC-focused job duties
5	**SCIP refresh.** SCIP is a living document that continues to be executed in a timely manner. Updated SCIPs are reviewed and approved by SIGB/SIEC.	No SCIP OR SCIP older than 3 years	SCIP updated within last 2 years	SCIP updated in last 2 years and progress made on >50% of goals
6	**SCIP strategic goal percentage.** SCIP goals are primarily strategic to improve long term emergency communications ecosystem (LMR, LTE, 9-1-1, A&W) and future technology transitions (5G, IoT, UAS, etc.). (Strategic and non-strategic goals are completely different; strategy – path from here to the destination; it is unlike tactics which you can "touch"; cannot "touch" strategy)	<50% are strategic goals in SCIP	>50%<90% are strategic goals in SCIP	>90% are strategic goals in SCIP

Marker	Best Practices / Performance Markers	Initial	Defined	Optimized
7	**Integrated emergency communication grant coordination.** Designed to ensure state / territory is tracking and optimizing grant proposals, and there is strategic visibility how grant money is being spent.	No explicit approach or only informal emergency communications grant coordination between localities, agencies, SAA and/or the SWIC within a state / territory	SWIC and/or SIGB provides guidance to agencies and localities for emergency communications grant funding but does not review proposals or make recommendations	SWIC and/or SIGB provides guidance to agencies and localities for emergency communications grant funding and reviews grant proposals for alignment with the SCIP. SWIC and/or SIGB provides recommendations to the SAA
8	**Communications Unit process.** Communications Unit process present in state / territory to facilitate emergency communications capabilities. Check the boxes of which Communications positions are currently covered within your process: ☐ COML ☐ COMT ☐ ITSL ☐ RADO ☐ INCM ☐ INTD ☐ AUXCOM ☐ TERT	No Communications Unit process at present	Communications Unit process planned or designed (but not implemented)	Communications Unit process implemented and active
9	**Interagency communication.** Established and applied interagency communications policies, procedures, and guidelines.	Some interoperable communications SOPs/SOGs exist within the area and steps have been taken to institute these interoperability procedures among some agencies	Interoperable communications SOPs/SOGs are formalized and in use by agencies within the area. Despite minor issues, SOPs/SOGs are successfully used during responses and/or exercises	Interoperable communications SOPs/SOGs within the area are formalized and regularly reviewed. Additionally, NIMS procedures are well established among agencies and disciplines. All needed procedures are effectively utilized during responses and/or exercises.
10	**TICP (or equivalent) developed.** Tactical Interoperable Communications Plans (TICPs) established and periodically updated to include all public safety communications systems available	Regional or statewide TICP in place	Statewide or Regional TICP(s) updated within past 2-5 years	Statewide or Regional TICP(s) updated within past 2 years
11	**Field Operations Guides (FOGs) developed.** FOGs established for a state or territory and	Regional or statewide FOG in place	Statewide or Regional FOG(s) updated within past 2-5 years	Statewide or Regional FOG(s) updated within past 2 years

Marker	Best Practices / Performance Markers	Initial	Defined	Optimized
	periodically updated to include all public safety communications systems available			
12	**Alerts & Warnings.** State or Territory has Implemented an effective A&W program to include Policy, Procedures and Protocol measured through the following characteristics: (1) Effective documentation process to inform and control message origination and distribution (2) Coordination of alerting plans and procedures with neighboring jurisdictions (3) Operators and alert originators receive periodic training (4) Message origination, distribution, and correction procedures in place	<49% of originating authorities have all of the four A&W characteristics	>50%<74% of originating authorities have all of the four A&W characteristics	>75%<100% of originating authorities have all of the four A&W characteristics
13	**Radio programming.** Radios programmed for National/Federal, SLTT interoperability channels and channel nomenclature consistency across a state / territory.	<49% of radios are programed for interoperability and consistency	>50%<74% of radios are programed for interoperability and consistency	>75%<100% of radios are programed for interoperability and consistency
14	**Cybersecurity Assessment Awareness.** Cybersecurity assessment awareness. (Public safety communications networks are defined as covering: LMR, LTE, 9-1-1, and A&W)	Public safety communications network owners are aware of cybersecurity assessment availability and value (check yes or no for each option) ☒ LMR ☒ LTE ☒ 9-1-1/CAD ☒ A&W	Initial plus, conducted assessment, conducted risk assessment. (Check yes or no for each option) ☐ LMR ☐ LTE ☐ 9-1-1/CAD ☐ A&W	Defined plus, Availability of Cyber Incident Response Plan (check yes or no for each option) ☐ LMR ☐ LTE ☐ 9-1-1/CAD ☐ A&W
15	**NG9-1-1 implementation.** NG9-1-1 implementation underway to serve state / territory population.	Working to establish NG9-1-1 governance through state/territorial plan. • Developing GIS to be able to support NG9-1-1 call routing. • Planning or implementing ESInet and Next Generation Core Services (NGCS). • Planning to or have updated PSAP equipment to handle	More than 75% of PSAPs and Population Served have: • NG9-1-1 governance established through state/territorial plan. • GIS developed and able to support NG9-1-1 call routing. • Planning or implementing ESInet and Next Generation Core Services (NGCS).	More than 90% of PSAPs and Population Served have: • NG9-1-1 governance established through state/territorial plan. • GIS developed and supporting NG9-1-1 call routing. • Operational Emergency Services IP Network

Marker	Best Practices / Performance Markers	Initial	Defined	Optimized
		basic NG9-1-1 service offerings.	• PSAP equipment updated to handle basic NG9-1-1 service offerings.	(ESInet)/Next Generation Core Services (NGCS). • PSAP equipment updated and handling basic NG9-1-1 service offerings.
16	**Data operability / interoperability.** Ability of agencies within a region to exchange data on demand, and needed, and as authorized. Examples of systems would be: - CAD to CAD - Chat - GIS - Critical Incident Management Tool (- Web EOC)	Agencies are able to share data only by email. Systems are not touching or talking.	Systems are able to touch but with limited capabilities. One-way information sharing.	Full system to system integration. Able to fully consume and manipulate data.
18	**Communications Exercise objectives.** Specific emergency communications objectives are incorporated into applicable exercises Federal / state / territory-wide	Regular engagement with State Training and Exercise coordinators	Promote addition of emergency communications objectives in state/county/regional level exercises (target Emergency Management community). Including providing tools, templates, etc.	Initial and defined plus mechanism in place to incorporate and measure communications objectives into state/county/regional level exercises
19	**Trained Communications Unit responders.** Communications Unit personnel are listed in a tracking database (e.g., NQS One Responder, CASM, etc.) and available for assignment/response.	<49% of public safety agencies within a state / territory have access to Communications Unit personnel who are listed in a tracking database and available for assignment/response	>50%<74% of public safety agencies within a state / territory have access to Communications Unit personnel who are listed in a tracking database and available for assignment/response	>75%<100% of public safety agencies within a state / territory have access to Communications Unit personnel who are listed in a tracking database and available for assignment/response
20	**Communications Usage Best Practices/Lessons Learned.** Capability exists within jurisdiction to share best practices/lessons learned (positive and/or negative) across all lanes of the Interoperability Continuum related to all components of the emergency communications ecosystem	Best practices/lessons learned intake mechanism established. Create Communications AAR template to collect best practices	Initial plus review mechanism established	Defined plus distribution mechanism established
21	**Wireless Priority Service (WPS) subscription.** WPS penetration across state / territory compared to maximum potential	<9% subscription rate of potentially eligible participants who signed up WPS across a state / territory	>10%<49% subscription rate of potentially eligible participants who signed up for WPS a state / territory	>50%<100% subscription rate of potentially eligible participants who signed up for WPS across a state / territory
22	**Outreach.** Outreach mechanisms in place to share information across state	SWIC electronic communication (e.g., SWIC email, newsletter,	Initial plus web presence containing information about	Defined plus in-person/webinar conference/meeting attendance

Marker	Best Practices / Performance Markers	Initial	Defined	Optimized
		social media, etc.) distributed to relevant stakeholders on regular basis	emergency communications interoperability, SCIP, trainings, etc.	strategy and resources to execute
23	**Sustainment assessment.** Identify interoperable component system sustainment needs;(e.g., communications infrastructure, equipment, programs, management) that need sustainment funding. (Component systems are emergency communications elements that are necessary to enable communications, whether owned or leased - state systems only)	< 49% of component systems assessed to identify sustainment needs	>50%<74% of component systems assessed to identify sustainment needs	>75%<100% of component systems assessed to identify sustainment needs
24	**Risk identification.** Identify risks for emergency communications components. (Component systems are emergency communications elements that are necessary to enable communications, whether owned or leased. Risk Identification and planning is in line with having a communications COOP Plan)	< 49% of component systems have risks assessed through a standard template for all technology components	>50%<74% of component systems have risks assessed through a standard template for all technology components	>75%<100% of component systems have risks assessed through a standard template for all technology components
25	**Cross Border / Interstate (State to State) Emergency Communications.** Established capabilities to enable emergency communications across all components of the ecosystem.	Initial: Little to no established: ☒ Governance ☒ SOPs/MOUs ☒ Technology ☒ Training/Exercises ☒ Usage	Defined: Documented/established across some lanes of the Continuum: ☐ Governance ☒ SOPs/MOUs ☒ Technology ☐ Training/Exercises ☒ Usage	Optimized: Documented/established across all lanes of the Continuum: ☐ Governance ☐ SOPs/MOUs ☐ Technology ☐ Training/Exercises ☐ Usage

APPENDIX B: ACRONYMS

Acronym	Definition
AAR	After-Action Report
AUXCOMM/AUXC	Auxiliary Emergency Communications
A&W	Alerts and Warnings
BITS	Department of Administrative Services – Bureau of Information and Technology Services
CASM	Communication Assets Survey and Mapping
CISA	Cybersecurity and Infrastructure Security Agency
CLMRN	Connecticut Land Mobile Radio Network
COML	Communications Unit Leader
CTS	Connecticut Telecommunications Service, Technical unit of DESPP Division of Emergency Telecommunications charged with technical planning and operations of CLMRN
COMT	Communications Unit Technician
COMU	Communications Unit Program
COOP	Continuity of Operations Plan
CPSICEC	Connecticut Public Safety Interoperable Communications Executive Committee
CTALERT	Connecticut Alert
CMED	Centralized Medical Emergency Direction System
DHS	Department of Homeland Security
DEMHS	Division of Emergency Management and Homeland Security (Division of DESPP)
DESPP	Department of Emergency Services and Public Protection
DSET	Division of Statewide Emergency Telecommunications (Division of DESPP)
ESInet	Emergency Services Internal Protocol Network
EMPG	Emergency Management Performance Grant
FOG	Field Operations Guide
GIS	Geospatial Information System
ICTAP	Interoperable Communications Technical Assistance Program
INCM	Incident Communications Center Manager
INTD	Incident Tactical Dispatcher
IP	Internet Protocol
IPAWS	Integrated Public Alerts and Warning System
ITSL	Information Technology Service Unit Leader
LMR	Land Mobile Radio
MHz	Megahertz
MOU	Memorandum of Understanding
NSWIC	National Council of Statewide Interoperability Coordinators
NECP	National Emergency Communications Plan

Acronym	Definition
NEMA	National Emergency Management Association
NESEC	Northeast States Emergency Consortium
NIMS	National Incident Management System
NG9-1-1	Next Generation 9-1-1
PSAC	Public Safety Advisory Committee
PSAP	Public Safety Answering Point
RADO	Radio Operator
RECCWG	Regional Emergency Communications Coordination Working Groups
SCIP	Statewide Communication Interoperability Plan
SLA	State and Local Assistance
SOP	Standard Operating Procedure
SWIC	Statewide Interoperability Coordinator
TA	Technical Assistance
TERT	Telecommunications Emergency Response Team
TICP	Tactical Interoperable Communications Plan
WPS	Wireless Priority Service