NORTH CAROLINA STRATEGIC COMMUNICATION INTEROPERABILITY PLAN

January 2025

Developed by the Statewide Interoperability 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

Greetings,

As the Statewide Interoperability Coordinator (SWIC) for North Carolina, I am pleased to present to you the 2025 North Carolina Strategic 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 Statewide Interoperability Executive Committee (SIEC) collaborated 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, cybersecurity, and funding. They are designed to support our state in planning for emerging technologies and navigating the ever-changing emergency communications ecosystem. They also incorporate many topics, concepts, and technology gaps that were identified during Hurricane Helene. These gaps put a greater importance on working through the provided improvement plan.

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

Sincerely,

Greg Hauser
North Carolina Statewide Interoperability Coordinator
North Carolina Department of Public Safety
Division of Emergency Management

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 North Carolina'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 North Carolina 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 North Carolina along with methods and strategies for funding sustainment and enhancement to meet long-term goals.
- **Implementation Plan** – Describes North Carolina's plan to implement, maintain, and update the SCIP to enable continued evolution of and progress toward the state's interoperability goals.

The SCIP is intended to compliment and/or align with all other strategic plans that address public safety communications to help create a unified vision for stakeholders. These include but are not limited to:

- National Emergency Communications Plan (NECP) (Department of Homeland Security)
- North Carolina State 911 Plan (NCDIT 911 Board)
- North Carolina Emergency Support Function (ESF) 2 Plan (NCEM Communications)
- North Carolina Homeland Security Strategy (NCEM Homeland Security)
- North Carolina Threat and Hazard Identification and Risk Assessment (NCEM Infrastructure)
- North Carolina State Emergency Communications Committee (SECC) Emergency Alerting System (EAS) plan

The Emergency Communications Ecosystem consists of many inter-related components and functions, including communications for incident response operations, notifications and 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] and highlighted below.

The Emergency Communications Ecosystem consists of the following components.

1. **Reporting and Requesting Assistance (Public to Government)**. The includes 911, 311, tip lines and applications, telematics, social media, web applications, and other methods that the public uses to engage public safety processes.
2. **Incident Coordination and Response (Government to Government).** This component contains the traditional interoperability methods for which public safety and first responders have engaged in for numerous years. This includes information sharing and collaboration, land mobile radio communications, usage guidelines, training and exercising and other operational aspects of first responders' ability to react and respond to reports and requests for assistance.
3. **Alerts, Warnings, and Notifications (Government to Public).** This includes government entities and their ability to alert and warn groups of people of active threats, civil dangers, hazardous materials incidents, AMBER alerts, weather warnings, fire danger and other instances where people need to take action to save lives or property.
4. **Public Interaction (Public to Public).** This component focuses on the public's use of commercial wireline and wireless communications networks to engage in daily activities under a no stress environment.

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.

[1] 2019 National Emergency Communications Plan
[2] Interoperability Continuum Brochure

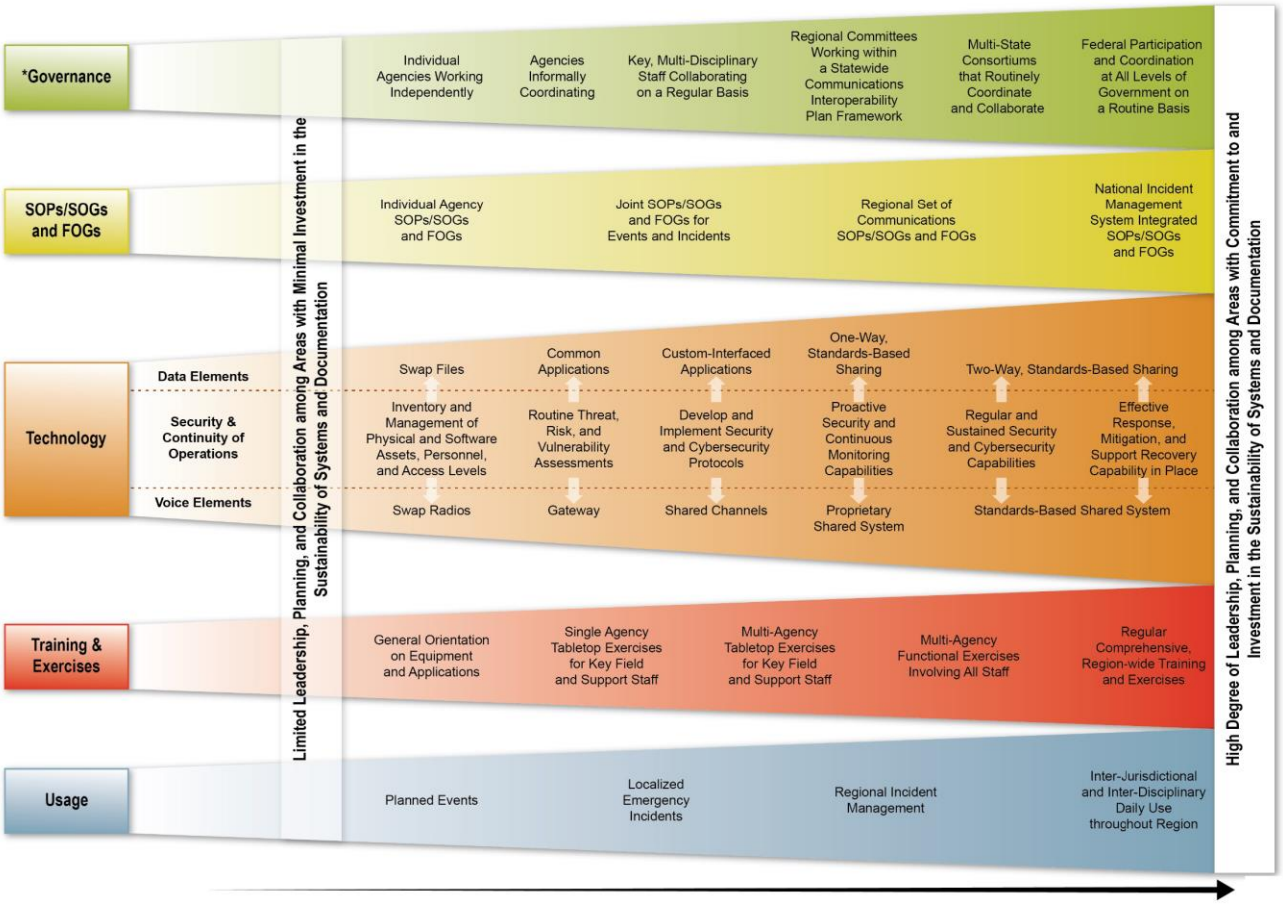

Figure 1: Interoperability Continuum

Interoperability and Emergency Communications Overview

North Carolina defines interoperability as the process of building and sustaining trust among stakeholders to effectively implement and maintain processes, technologies, training, exercises, and usage for exchanging voice and data as needed. 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. Relationship building in a

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.

Fostering and building relationships amongst the emergency communications ecosystem is the highest priority for North Carolina emergency communications stakeholders. The SIEC is charged with breaking down silos and creating a realistic focus on both operability and interoperability challenges. Technology cannot solve human interoperability issues and understanding this will provide first responder communications stakeholders a safe environment to focus directly on each individual challenge without the fear of harm or retribution.

VISION AND MISSION

This section describes North Carolina's vision and mission for improving emergency and public safety communications interoperability:

Vision:

To promote the most efficient, effective, and secure means of operable and interoperable communications between all entities involved in public safety in North Carolina

Mission:

Provide strategic guidance to the whole response community to mitigate loss of life and property through public safety communications operability and interoperability planning and coordination

GOVERNANCE

The State Emergency Response Commission (SERC), a body appointed by the Governor, provides public safety recommendations and guidance to stakeholders. Under the SERC, the State Interoperability Executive Committee (SIEC) operates as a formal subcommittee, tasked with developing the SCIP and offering expertise on interoperable communications. North Carolina Emergency Management (NCEM), specifically the SWIC, is charged with executive direction of the SIEC. The North Carolina SIEC facilitates the flow of planning best practices and policy recommendations among local, regional, and state communities concerning public safety communications. North Carolina's regions are organized into Domestic Preparedness Regions (DPRs) for Homeland Security planning, where gaps and capabilities are identified. Representation within these DPRs assist with homeland security grant projects, and the SIEC includes three DPR members: one representing Eastern NC (DPRs 1, 2, 3), one for Central NC (DPRs 4, 5, 6), and one for Western NC (DPRs 7, 8, 9). The North Carolina State Highway Patrol (NCSHP) oversees the VIPER System, which serves over 198,000 users across 64 counties daily, with SIEC representatives from the Technical Services Unit and local Land Mobile Radio (LMR) administrators. The NC Department of Information Technology's Broadband Infrastructure Office hosts the State Point of Contact (SPOC) for FirstNet and public safety broadband coordination, advocating for North Carolina's responders, and the SIEC includes representatives from the Broadband Infrastructure Office and FirstTech. Additionally, the North Carolina 911 Board, established by North Carolina General Statute 143B-1401, manages wireline and wireless 911 call delivery, related policies and procedures, and the administration of the state's 911 Fund, with one 911 Board staff representative serving on the SIEC. Further explanation on all representatives and SIEC specifics are outlined in the North Carolina SIEC Charter.

The North Carolina SIEC plans to strengthen partnerships with federal, state, tribal, and local agencies while engaging neighboring states and other communications entities both public and private sector. The SIEC also seeks to engage the general assembly, either directly, or through the

SERC, more broadly and include follow-on support for emergency communications initiatives identified by its membership.

North Carolina's emergency communications governance map is depicted in Figure 2.

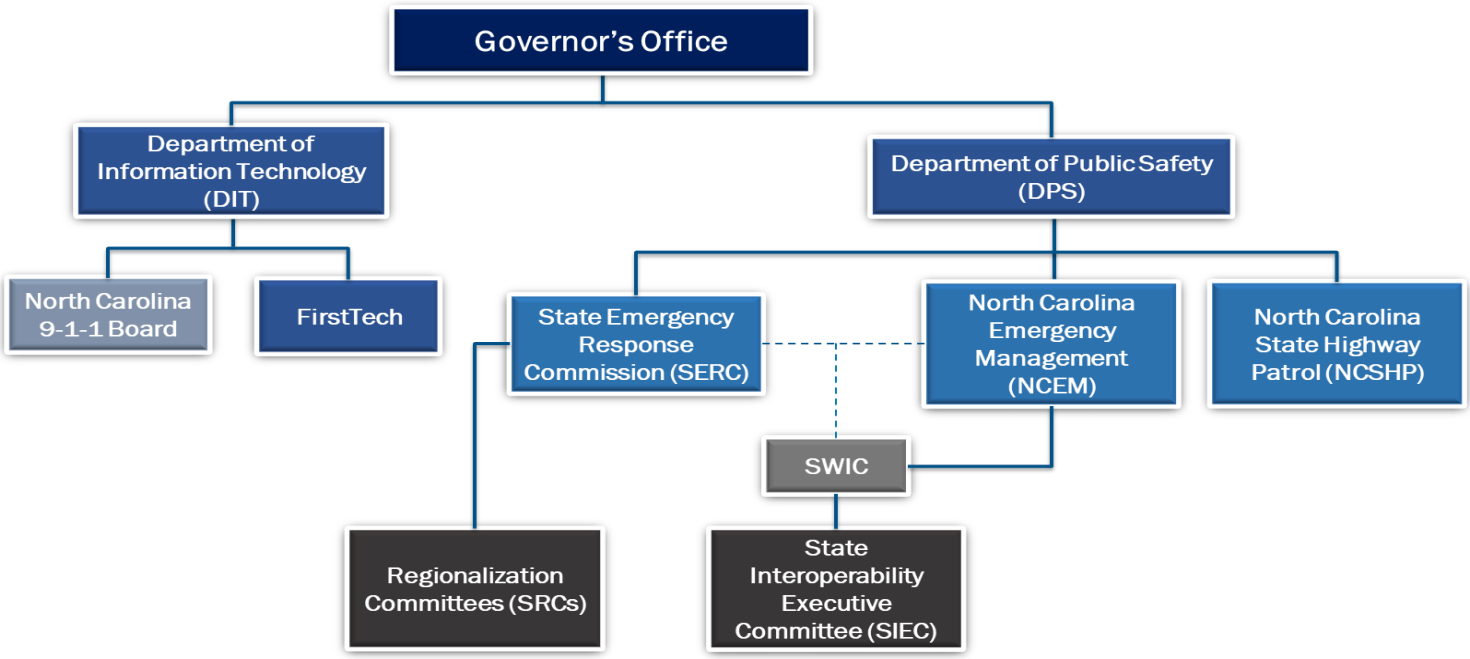

Figure 2: North Carolina's Emergency Communications Governance Map

Governance goals and objectives include the following:

Governance	
Goals	**Objectives**
1. Formally recognize the SIEC as the operational policy advisor to VIPER.	1.1 Update the SIEC charter to adopt a recognition of the SIEC as an operational policy advisor to VIPER.
	1.2 Support VIPER technology sustainment, advancement, resiliency, physical security, cybersecurity, and funding efforts.
2. Provide public safety communications education and outreach.	2.1 Request and participate in CISA provided technical assistance (TA).
	2.2 Encourage stakeholder engagement with the SWIC and SIEC to share feedback and situational awareness.
	2.3 Establish SIEC sub-committee to develop and implement virtual stakeholder engagement opportunities (i.e., panels, presentations, etc.).

Goals	Objectives
	2.4 Collaborate with state and local institutions to promote academic, hiring, and professional development opportunities.
	2.5 Expand training and outreach beyond ICT courses
	2.6 Incorporate communications into trainings and exercises more frequently. a. Develop and incorporate standard operational communication injects.

TECHNOLOGY AND CYBERSECURITY

Land Mobile Radio

The North Carolina State Highway Patrol (NCSHP) manages the North Carolina VIPER System, which serves 198,000 users across 64 counties daily. The State Interoperability Executive Committee (SIEC) includes representatives from the Technical Services Unit and local Land Mobile Radio (LMR) administrators. VIPER, a statewide 800-megahertz (MHz) Project 25 (P25) mission-critical radio system, provides access to all federal, state, and local agencies for seamless communication. As of December 2024, the network consists of 240 tower sites, over 198,000 subscriber IDs, and more than 350 agencies relying on VIPER daily. Additionally, there are 18 standalone P25 LMR systems and 18 standalone legacy (Non-P25) LMR systems at the local level in North Carolina. These standalone systems are encouraged, and to a large extent, have interoperability processes in place to address communications gaps.

North Carolina seeks to ensure that all public safety radios are programmed with the current Statewide interoperability template and have the capability of encryption as outlined in the State's encryption plan to address ongoing and future threats. Additionally, the goal is for all public safety radios to operate in a Time Division Multiple Access (TDMA) environment. The state aims to link the VIPER system with neighboring state systems while securing sustainable funding for maintenance, personnel, and upgrades. North Carolina seeks to include all Land Mobile Radio (LMR) system representatives, regardless of the manufacturer, and foster interstate collaboration between system owners. There is also a focus on increasing awareness of unauthorized access to LMR systems, with Link Layer Authentication being a potential solution, alongside more formalized governance of the VIPER system. Finally, the state strives to maintain cohesive interoperability across the VIPER system.

911

North Carolina has completed the process of implementing Next Generation 911 (NG911), with 124 Public Safety Answering Points (PSAPs). A NG911 plan was developed and approved in December 2023, and the Emergency Services Internet Protocol Network (ESInet) has been fully deployed statewide. The Network Monitoring and Assistance Center (NMAC) operates 24/7, providing continuous support. In August 2022, North Carolina completed the geospatial service for entities providing Geographic Information System (GIS) data to support call routing. By February 2024, the state connected Seymour Johnson Air Force Base to the statewide ESInet and continued

outreach to other military bases. There has been significant participation in CAD-to-CAD data-sharing solutions, and over 91% of PSAPs are now using hosted call-handling solutions. A tertiary wireless connection to the ESInet is being rolled out to improve PSAP resiliency, and encryption upgrades are being implemented to improve cyber resiliency.

Broadband

The North Carolina Department of Information Technology's First Responder Emerging Technologies (FirstTech) program is the state entity responsible for supporting the federal broadband effort and providing education and outreach on public safety broadband to first responder agencies at all levels of government across the state. The Division of Broadband and Digital Equity is represented on the Statewide Interoperability Executive Committee (SIEC) and provides valuable technical insight and support to stakeholders.

The desired state of public safety broadband in North Carolina includes expanded coverage across the state to ensure reliable communication for first responders. This effort involves investigating applications and services that are specifically applicable to their needs. There is also a focus on effectively defining and documenting critical infrastructure vulnerabilities to prepare for potential outages. Increased collaboration with wireline and wireless carriers is essential for improving public and private Emergency Support Function #2 (ESF #2) information sharing. Engaging more closely with the Division of Broadband and Digital Equity will help maximize broadband public safety projects, particularly to benefit rural public safety entities. Additionally, the SIEC will evaluate common statewide platforms, and a statewide model for applications will be developed to streamline and enhance public safety operations.

Alerts and Warnings

NCEM is currently the authorizing agency for the state's access to the Integrated Public Alert Warning System (IPAWS). IPAWS encompasses the Emergency Alert System (EAS), Wireless Emergency Alerts (WEA), and National Oceanic and Atmospheric Administration (NOAA) Weather Radio. Public alerting authorities in North Carolina include 49 county level, three (3) state level, one (1) tribal nation, and two (2) military installations. Many jurisdictions utilize social media, as well as state and local unique alerting systems and non-IPAWS opt-in alerting software.

The SIEC provides policy guidance to federal, state, tribal, and local public alerting authorities (PAA) detailing processes for on-boarding, creating, authorizing, and disseminating alerts and warnings. The advancement of alert and warning technology, including the integration of existing technology platforms will be a focus to ensure continuity and improve access to the public.

Cybersecurity

The SIEC recognizes the importance of cybersecurity and the role it plays in every component of the emergency communications ecosystem. Prioritizing cybersecurity planing, training, exercising and providing funding for emergency communications inititatives must be done to protect public safety technology platforms. Managing consequences related to cyber intrusions almost always lead to operability and interoperability gaps.

There is an established process in North Carolina for reporting cyber intrusions to local government entities, guided by current legislation that outlines necessary response actions. However, cybersecurity prevention efforts remain largely fragmented and independent, varying by level of

government. For example, support for Local PSAP cybersecurity is provided by the 911 Board to enhance their preparedness and resilience against potential cyber threat. The SIEC will work with the North Carolina Joint Cyber Task Force (NC JCTF) to provide subject matter expertise and help with information gathering and dissemination as requested.

Technology and cybersecurity goals and objectives include the following:

Technology and Cybersecurity	
Goals	**Objectives**
3. Promote the adoption of non-land mobile radio (LMR) technologies to expand emergency response capabilities.	3.1 Strengthen and maintain relationships with the vendor community.
	3.2 Promote discussion at SIEC meetings regarding emerging technology.
	3.3 Support research with PBS-NC on utilizing digital television to serve public safety dispatching/paging, information sharing, and public alerts and warnings.
	3.4 Leverage groups to evaluate and provide recommendations on expanding communications technology platforms and processes.
4. Continue the enhancement of interoperable LMR capabilities statewide.	4.1 Explore technologies to allow interstate and intrastate roaming/connectivity between disparate voice systems, to include non LMR systems.
	4.2 Require the adoption and verify the use of the required VIPER template.
	4.3 Maintain a list of allowable equipment and adjuncts.
5. Expand technologies that integrate with LMR systems and capabilities.	5.1 Encourage the evaluation and exploration of integrating non-LMR technologies into the LMR environment.
	5.2 Create a plan for the responsible integration of non-LMR technologies into the LMR environment.
6. Support sustainment, enhancement, and any other functions or processes related to PACE, COOP, and COG efforts.	6.1 Research tools and solutions for interoperability resource management and information sharing.
	6.2 Expand dispatch capabilities between jurisdictions during special events and disasters.
	6.3 Explore dispatch interoperability opportunities.
	6.4 Encourage the use and monitoring of “calling” and “hailing” frequencies (SW CALL) within emergency communication centers (ECCs) and public safety answering points (PSAPs) through education and training.
	6.5 Assist public safety agencies with primary, alternate, contingency, emergency (P.A.C.E.) planning.
	6.6 Assist state and local government entities with continuity of operations (COOP) and continuity of government (COG) planning, training, and exercising.

7. **Support the implementation of statewide technology available for local access to alerts and warnings platforms.**	7.1 Increase outreach and education to public safety agencies and the public on alerts and warnings.
	7.2 Explore interstate alerts and warnings opportunities.
	7.3 Expand alerts and warnings capabilities for public alerting authorities to include interaction with the deaf and hard of hearing community.
	7.4 Expand local capabilities to originate alerts and warnings.
	7.5 Research best practices to help standardize translations of multilingual messages.
8. **Prioritize physical and cybersecurity for communications ecosystem processes, pathways, and networks.**	8.1 Recommend adherence to security standards consistent with established national best practices and guidance.
	8.2 Continue cybersecurity and physical security assessments and improvements.
	8.3 Encourage training and adoption of cybersecurity best practices, to include state cybersecurity response plans and objectives.
	8.4 Continue to explore opportunities to increase awareness and assist where applicable for emergency communications ecosystem cyber health and hygiene.

FUNDING

Funding for emergency communications technology has declined over the past three (3) years. Emergency communications technology hardware and software costs have increased significantly over the past three (3) years. The inability for state, tribal, and local government entities to procure advancements in this technology has, is, and will continue to impact interoperability in North Carolina.

For example, all funding for the VIPER system in North Carolina is provided by the state legislature, however, there has been a reduction in general funds, federal grant funding, thus creating challenges for the continued rising costs of infrastructure and user end equipment. This funding gap makes it difficult for users of VIPER to purchase required upgrades to maintain their communication capabilities.

The SIEC membership organizations will explore options to increase funding availability at the local level for several critical needs, including equipment replacement, end-of-life radio, and computer equipment (such as radio consoles, mobile devices, desktop, and laptop computers), equipment upgrades, and the addition of Time Division Multiple Access (TDMA) and Advanced Encryption Standard-256 (AES-256) encryption capabilities to existing radios. They also aim to support emerging technologies, and the maintenance and sustainment of these capabilities. The SIEC's primary focus will be on aligning with federal and state grant requirements, ensuring equipment interoperability, and supporting training, exercises, alerts, and warning platforms. Additionally, the SWIC will work to attain funding to support planning and outreach meetings, training and exercise, and engagement with constituent organizations.

Funding goals and objectives include the following:

Goals	Objectives
9. Develop and maintain sustainable funding for public safety interoperable communications.	9.1 Develop an infrastructure sustainment business plan.
	9.2 Identify and share funding opportunities for encryption and lifecycle planning.
	9.3 Identify and address capability gaps, opportunities, and resource needs at the regional and local levels (i.e., caches, threat detection, etc.).
	9.4 Identify funding opportunities for the VIPER system to be sustainable for maintenance, personnel, and upgrades.
10. Assist local agencies to identify and request funding.	10.1 Support North Carolina State Highway Patrol (NCSHP) VIPER to identify county and local government users that can assist in requests to the General Assembly.
	10.2 Seek opportunities for outreach and education through associations (i.e., North Carolina County of Commissioners and North Carolina League of Municipalities) to educate the legislature on operable, interoperable, and sustainment communications priorities.
	10.3 Provide subject matter expertise on operable and interoperable sustainment elements of first responder communications.

TRAINING AND EXCERCISES

The SIEC supports all training and exercises that create an opportunity for first responders and members of the emergency communications ecosystem to test operability and interoperability policy, processes, equipment, and technology. The SIEC has been charged with certifying and credentialing information and communications technology (ICT) incident command system (ICS) positions by the NC all-hazards incident management team (AHIMT) committee who is charged with similar duties for non-ICT ICS positions.

The SIEC, working with the NCEM Communications Branch, will set ICT courses, continuing education, drills, and exercises. The SIEC can also provide SMEs for exercise planners, training course instructors, and any other group that wishes to facilitate tabletop, functional, or full-scale exercises.

Historically, law enforcement partners have taken a passive approach to incident and event-based communications interoperability. The SIEC strives to engage law enforcement and help train and educate key decision-makers to prevent basic interoperability gaps that have been corrected in other disciplines.

Training and exercises goals and objectives include the following:

Goals	Objectives
11. Continue to advance and strengthen the ICT program in the state.	11.1 Expand classroom training opportunities for ICT positions to include IT Services Unit positions as well as continue training the Communications Unit (COMU) positions.
	11.2 Review ICT position task books for validity and usefulness.
	11.3 Work with CISA and FEMA to prioritize the revision of COMU curriculum and move forward with new ICT position course curriculum.
12. Target training and education opportunities to entities with a history of communications and interoperability-based challenges in real world events.	12.1 Prioritize communications focused continuity of government training and education to both public safety and non-public safety government entities.
	12.2 Continue to educate stakeholders on the importance of adopting ICT as an ICS construct.
	12.3 Encourage law enforcement partners to engage in strategic and tactical communications planning for special events.

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.

North Carolina's implementation plan is shown in the table below.

Goals	Objectives	Owners	Completion Dates
1. **Formally recognize the SIEC as the operational policy advisor to VIPER.**	1.1 Update the SIEC charter to adopt a recognition of the SIEC as an operational policy advisor to VIPER.	Governance Working Group NCSHP	1.1 Q2 2025 SIEC Meeting 1.2 Ongoing
	1.2 Support VIPER technology sustainment, advancement, resiliency, physical security, cybersecurity, and funding efforts.		
2. **Provide public safety communications education and outreach.**	2.1 Request and participate in CISA provided technical assistance (TA).	SWIC Training and Exercise Working Group Ad-Hoc SMEs	2.1 Ongoing 2.2 Ongoing 2.3 Q3 2025 2.4 Ongoing 2.5 Ongoing 2.6 Ongoing
	2.2 Encourage stakeholder engagement with the SWIC and SIEC to share feedback and situational awareness.		
	2.3 Establish SIEC sub-committee to develop and implement virtual stakeholder engagement opportunities (i.e., panels, presentations, etc.).		
	2.4 Collaborate with state and local institutions to promote academic, hiring, and professional development opportunities.		
	2.5 Expand training and outreach beyond ICT courses		
	2.6 Incorporate communications into trainings and exercises more frequently. a. Develop and incorporate standard operational communication injects		

[3] Emergency Communications Technical Assistance Planning Guide

3. Promote the adoption of non-land mobile radio (LMR) technologies to expand emergency response capabilities.	3.1 Strengthen and maintain relationships with the vendor community.	SWIC Training and Exercise Working Group Governance Working Group	Ongoing
	3.2 Promote discussion at SIEC meetings regarding emerging technology.		
	3.3 Support research with PBS NC on utilizing digital television to serve public safety dispatching/paging, information sharing, and public alerts and warnings.		
	3.4 Leverage groups to evaluate and provide recommendations on expanding communications technology platforms and processes.		
4. Continue the enhancement of interoperable LMR capabilities statewide	4.1 Explore technologies to allow interstate and intrastate roaming/connectivity between disparate voice systems, to include non LMR systems.	SWIC Training and Exercise Working Group 911 Board Ad-Hoc SMEs	4.1 Ongoing 4.2 Ongoing 4.3 Q3 2025 4.4 Ongoing
	4.2 Require the adoption and verify the use of the required VIPER template.		
	4.3 Maintain a list of allowable equipment and adjuncts.		
5. Expand technologies that integrate with LMR systems and capabilities	5.1 Encourage the evaluation and exploration of integrating non-LMR technologies into the LMR environment.	SIEC Technology Working Group FirstTech Ad-Hoc SMEs	Ongoing
	5.2 Create a plan for the responsible integration of non-LMR technologies into the LMR environment.		

6. Support sustainment, enhancement, and any other functions or processes related to PACE, COOP, and COG efforts.	6.1 Research tools and solutions for interoperability resource management and information sharing.	Technology Working Group NCSHP	6.1 Ongoing 6.2 Q1 2026 6.3 Ongoing
	6.2 Expand dispatch capabilities between jurisdictions during special events and disasters.		
	6.3 Explore dispatch interoperability opportunities.		
	6.4 Encourage the use and monitoring of "calling" and "hailing" frequencies (SW CALL) within emergency communication centers (ECCs) and public safety answering points (PSAPs) through education and training.		
	6.5 Assist public safety agencies with primary, alternate, contingency, emergency (P.A.C.E.) planning.		
	6.6 Assist state and local government entities with continuity of operations (COOP) and continuity of government (COG) planning, training, and exercising.		
7. Support the implementation of statewide technology available for local access to alerts and warnings platforms.	7.1 Increase outreach and education to public safety agencies and the public on alerts and warnings.	Governance Working Group Technology Working Group NCSHP Ad-Hoc SMEs	7.1 Ongoing 7.2 Q3 2025
	7.2 Explore interstate alerts and warnings opportunities.		
	7.3 Expand alerts and warnings capabilities for public alerting authorities to include interaction with the deaf and hard of hearing community.		
	7.4 Expand local capabilities to originate alerts and warnings.		
	7.5 Research best practices to help standardize translations of multilingual messages.		

8. Prioritize physical and cybersecurity for communications ecosystem processes, pathways, and networks.	8.1 Recommend adherence to security standards consistent with established national best practices and guidance.	SWIC SIEC 911 Board FirstTech Ad-Hoc SMEs	Ongoing (initial planning session by Q2 2025)
	8.2 Continue cybersecurity and physical security assessments and improvements.		
	8.3 Encourage training and adoption of cybersecurity best practices, to include state cybersecurity response plans and objectives.		
	8.4 Continue to explore opportunities to increase awareness and assist where applicable for emergency communications ecosystem cyber health and hygiene.		
9. Develop and maintain sustainable funding for public safety interoperable communications.	9.1 Develop an infrastructure sustainment business plan.	SIEC Alerts and Warnings Working Group NCEM NCSHP	Ongoing
	9.2 Identify and share funding opportunities for encryption and lifecycle planning.		
	9.3 Identify and address capability gaps, opportunities, and resource needs at the regional and local levels (i.e., caches, threat detection, etc.).		
	9.4 Identify funding opportunities for the VIPER system to be sustainable for maintenance, personnel, and upgrades.		
10. Assist local agencies to identify and request funding.	10.1 Support North Carolina State Highway Patrol (NCSHP) VIPER to identify county and local government users that can assist in requests to the General Assembly.	Training and Exercise Working Group Joint Cyber Task Force 911 Board ECC CSA	Ongoing (initial planning session by Q2 2025)
	10.2 Seek opportunities for outreach and education through associations (i.e., North Carolina County of Commissioners and North Carolina League of Municipalities) to educate the legislature on operable, interoperable, and sustainment communications priorities.		
	10.3 Provide subject matter expertise on operable and interoperable sustainment elements of first responder communications.		

11. Continue to advance and strengthen the ICT program in the state.	11.1 Expand classroom training opportunities for ICT positions to include IT Services Unit positions as well as continue training the Communications Unit (COMU) positions.	SWIC NCEM Ad-Hoc SMEs	11.1 Q3 2025 11.2 Ongoing 11.3 Ongoing
	11.2 Review ICT position task books for validity and usefulness.		
	11.3 Work with CISA and FEMA to prioritize the revision of COMU curriculum and move forward with new ICT position course curriculum.		
12. Target training and education opportunities to entities with a history of communications and interoperability-based challenges in real world events.	12.1 Prioritize communications focused continuity of government training and education to both public safety and non-public safety government entities.	SIEC SWIC Ad-Hoc SMEs	12.1 Q3 2025 12.2 Ongoing 12.3 Ongoing
	12.2 Continue to educate stakeholders on the importance of adopting ICT as an ICS construct.		
	12.3 Encourage law enforcement partners to engage in strategic and tactical communications planning for special events.		

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 North Carolina assessment of their progress against the markers as of 09/16/2024

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 ☐ 911 ☐ Alerts, Warnings and Notifications	Defined (3-4) Governance body participation includes: ☐ Communications Champion/SWIC ☐ LMR ☐ Broadband/LTE ☐ 911 ☐ Alerts, Warnings and Notifications	Optimized (5) Governance body participation includes: ☒ Communications Champion/SWIC ☒ LMR ☒ Broadband/LTE ☒ 911 ☒ 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, 911, 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
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

Marker	Best Practices / Performance Markers	Initial	Defined	Optimized
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 periodically updated to include all public safety communications systems available	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
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	<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

Marker	Best Practices / Performance Markers	Initial	Defined	Optimized
	channel nomenclature consistency across a state / territory.			
14	**Cybersecurity Assessment Awareness.** Cybersecurity assessment awareness. (Public safety communications networks are defined as covering: LMR, LTE, 911, 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 ☐ 911/CAD ☐ A&W	Initial plus, conducted assessment, conducted risk assessment. (Check yes or no for each option) ☐ LMR ☐ LTE ☐ 911/CAD ☐ A&W	Defined plus, Availability of Cyber Incident Response Plan (check yes or no for each option) ☒ LMR ☒ LTE ☒ 911/CAD ☒ A&W
15	**NG911 implementation.** NG911 implementation underway to serve state / territory population.	Working to establish NG911 governance through state/territorial plan. • Developing GIS to be able to support NG911 call routing. • Planning or implementing ESInet and Next Generation Core Services (NGCS). • Planning to or have updated PSAP equipment to handle basic NG911 service offerings.	More than 75% of PSAPs and Population Served have: • NG911 governance established through state/territorial plan. • GIS developed and able to support NG911 call routing. • Planning or implementing ESInet and Next Generation Core Services (NGCS). • PSAP equipment updated to handle basic NG911 service offerings.	More than 90% of PSAPs and Population Served have: • NG911 governance established through state/territorial plan. • GIS developed and supporting NG911 call routing. • Operational Emergency Services IP Network (ESInet)/Next Generation Core Services (NGCS). • PSAP equipment updated and handling basic NG911 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	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

Marker	Best Practices / Performance Markers	Initial	Defined	Optimized
	Continuum related to all components of the emergency communications ecosystem			
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, social media, etc.) distributed to relevant stakeholders on regular basis	Initial plus web presence containing information about emergency communications interoperability, SCIP, trainings, etc.	Defined plus in-person/webinar conference/meeting attendance 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
AES-256	Advanced Encryption Standard-256
AUXC	Auxiliary Emergency Communications
A&W	Alerts and Warnings
CISA	Cybersecurity and Infrastructure Security Agency
COG	Continuity of Government
COML	Communications Unit Leader
COMT	Communications Unit Technician
COMU	Communications Unit Program
COOP	Continuity of Operations Plan
DHS	Department of Homeland Security
DPR	Domestic Preparedness Region
EAS	Emergency Alert System
ECC	Emergency Communications Center
ESF	Emergency Support Function
ESInet	Emergency Services Internal Protocol Network
FOG	Field Operations Guide
GIS	Geospatial Information System
ICT	Information and Communications Technology
ICTAP	Interoperable Communications Technical Assistance Program
IPAWS	Integrated Public Alert and Warning System
INTD	Incident Tactical Dispatcher
IP	Internet Protocol
ITSL	Information Technology Service Unit Leader
JCTF	Joint Cybersecurity Task Force
LMR	Land Mobile Radio
MHz	Megahertz
MOU	Memorandum of Understanding
NCDIT	North Carolina Department of Information Technology
NCEM	North Carolina Emergency Management
NCSHP	North Carolina State Highway Patrol
NCSWIC	National Council of Statewide Interoperability Coordinators
NECP	National Emergency Communications Plan
NG911	Next Generation 911
NMAC	National Mutual Aid Committee
NOAA	National Oceanic and Atmospheric Administration

Acronym	Definition
PSAP	Public Safety Answering Point
P25	Project 25
SCIP	Strategic Communication Interoperability Plan
SECC	State Emergency Communications Committee
SERC	State Emergency Response Commission
SME	Subject Matter Expert
SOG	Standard Operating Guidelines
SOP	Standard Operating Procedure
SPOC	State Point of Contact
SWIC	Statewide Interoperability Coordinator
TA	Technical Assistance
TDMA	Time Division Multiple Access
TERT	Telecommunications Emergency Response Team
TICP	Tactical Interoperable Communications Plan
WEA	Wireless Emergency Alerts
WPS	Wireless Priority Service
VIPER	Voice Interoperability Plan for Emergency Responders