INDIANA
STATEWIDE COMMUNICATION INTEROPERABILITY PLAN

November 2024

Developed by the Integrated Public Safety Commission with support from the Cybersecurity and Infrastructure Security Agency

DRAFT – INTERNAL WORKING DOCUMENT

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

Letter from the Statewide Interoperability Coordinator **1**
Introduction **2**
Interoperability and Emergency Communications Overview 3
Vision and Mission **4**
Governance **4**
Technology and Cybersecurity **7**
Land Mobile Radio 7
911 8
Broadband 9
Alerts and Warnings 9
Cybersecurity 10
Funding **12**
Implementation Plan **14**
Appendix A: State Markers **17**
Appendix B: Acronyms **21**

LETTER FROM THE STATEWIDE INTEROPERABILITY COORDINATOR

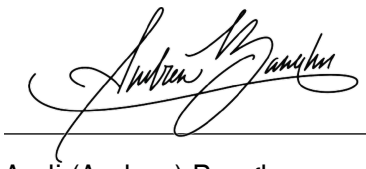
Greetings,

As the Statewide Interoperability Coordinator (SWIC) for Indiana, I am pleased to present the 2024 Indiana Statewide Communication Interoperability Plan (SCIP). This SCIP represents Indiana's continued commitment to improving emergency communications interoperability and supporting the public safety practitioners throughout Indiana. This SCIP update also meets current U.S. Department of Homeland Security grant guidelines.

Emergency communication stakeholders across Indiana, led by members of the Statewide Interoperability Executive (Council SIEC), collaborated to update this SCIP with actionable and measurable goals and objectives that have champions and deadlines identified to ensure completion. These goals and objectives incorporate the National Emergency Communications Plan (NECP) focusing on governance, technology, cybersecurity, and funding. Goals and objectives are designed to inspire our state in planning for emerging technologies and navigating the ever-changing emergency communications landscape in and surrounding Indiana. SCIP goals also incorporate parts of the SAFECOM/National Council of Statewide Interoperability Coordinators (NCSWIC) State Interoperability Markers, describing Indiana's level of interoperability maturity by measuring progress against these 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,



Andi (Andrea) Baughn
Indiana Statewide Interoperability Coordinator
Integrated Public Safety Commission

INTRODUCTION

The Indiana SCIP is a three-year strategic planning document containing 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 Indiana's emergency communication stakeholder's vision and mission for improving emergency and public safety communications interoperability over the next three-years.
- **Governance** – The SCIP is a guiding document and does not create any authority or direction over any state or local systems or agencies. However, the SCIP does describe the current governance mechanisms for communications interoperability within Indiana as well as successes, challenges, and priorities for improving it.
- **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 Indiana along with methods and strategies for funding sustainment and enhancement to meet long-term goals.
- **Implementation Plan** – Describes Indiana'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 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]

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] This tool identifies five critical success elements that must be addressed to achieve a sophisticated interoperability solution: governance, standard operating procedures (SOPs)/standard operating guidelines (SOGs) and field operations guides (FOGs), technology, training and exercises, and usage of interoperable communications. Jurisdictions across the Nation can use the Interoperability Continuum to track progress in strengthening interoperable communications.

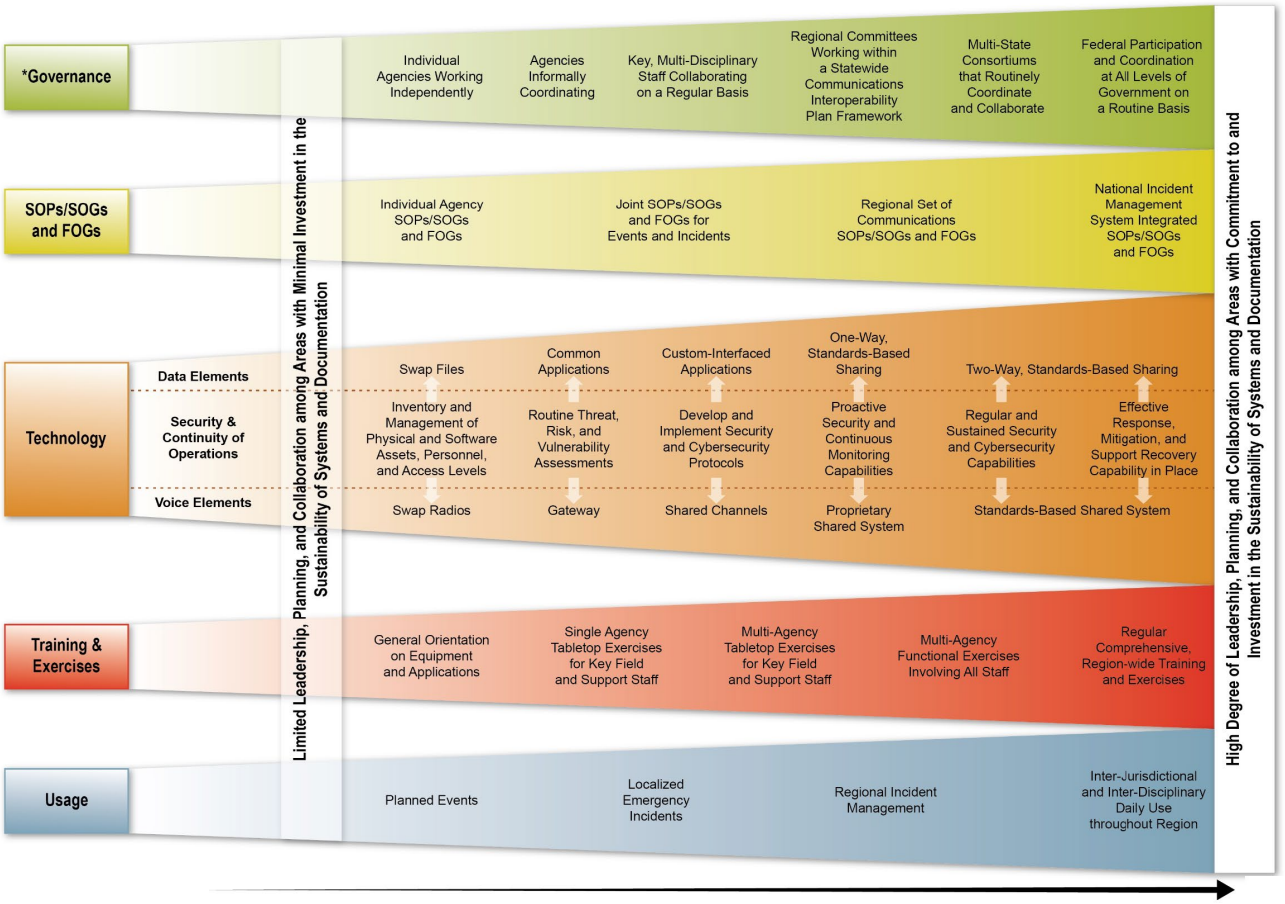


Figure 1: Interoperability Continuum

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 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.

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

Traditional voice capabilities, such as land mobile radio (LMR) and landline 911 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.

VISION AND MISSION

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

Vision:

Indiana's first responders will be able to leverage and share data and communicate at optimal efficiency, in real time, across jurisdictions and disciplines, enabling more effective response during day-to-day operations and catastrophic events.

Mission:

Indiana's mission is to facilitate statewide public safety communications and strengthen community safety and security by minimizing the barriers to interoperable communications.

GOVERNANCE

Indiana Code 5-26-2 established the Integrated Public Safety Commission (IPSC), the governing body for interoperable public safety communications in Indiana. The Commission is made up of 12 members that represent state and local agencies as well as private sector and legislative representatives appointed by the Governor.[3]

The Statewide Interoperability Executive Committee (SIEC) is a formal advisory committee to the SWIC, who chairs the committee, and is made up of members from each of the 10 state Homeland Security Districts and state agency partners and non-governmental agencies. The SIEC meets quarterly to discuss gaps in interoperable communications technology and provides a driving force for IPSC. SIEC includes two working groups: the Technology Working Group and the ICT Group. The Technology Working Group also has a Programming Sub-Committee to discuss several topics, including but not limited to the best practices for programming radios to the recommended interoperable template provided by IPSC. The ICT Group supports disaster response and communications as well as planning for large scale events.

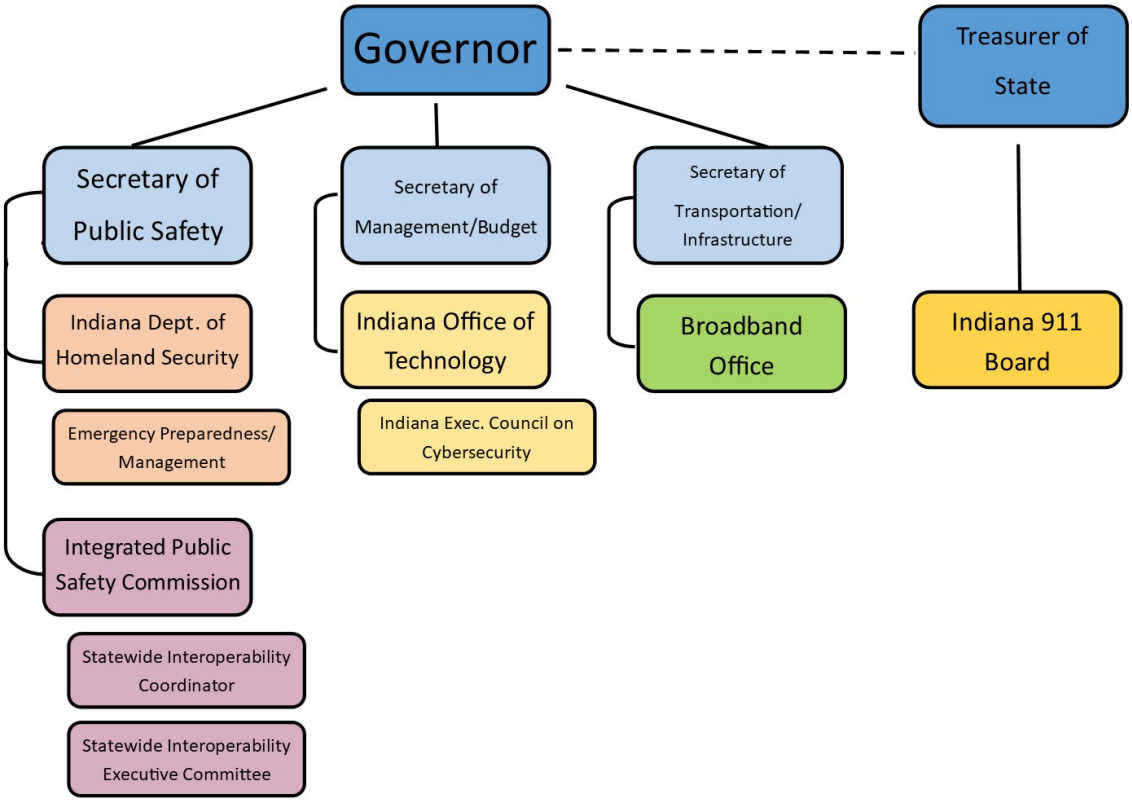
During Indiana's SCIP process, emergency communications stakeholders identified various challenges:

[3] Indiana Code 5-26-2

- Interoperability with the neighboring states
- Emerging technologies with unforeseen interoperability or interface issues, presenting challenges for state level encryption and intrastate interoperability.
- Growing need for IPSC System Training
    - IPSC provides Training and Outreach Coordinators to act as liaisons to assist local, state and federal agencies with their interoperability concerns, challenges, goals and requirements
    - Training is provided but not utilized by many users
- Turnover in local personnel leading to gaps in understanding of the statewide radio system
    - Knowledge is not being passed down during transitions impacting the development and maintenance of radio programming skills
- Standardized programming of interoperability talkgroups and channels
    - Standardized naming conventions
- Addressing subscriber unit programming gaps
    - Improving cross-state communications in the changing technology landscape, such as partnerships with Michigan and Kentucky
        - County public safety encountering incompatible systems with other neighboring states

The Indiana Department of Homeland Security (IDHS) and the Indiana State 911 Board hold voting positions on the SIEC. The Indiana Office of Technology is not directly involved in emergency communications governance but may increase their role in the future. Indiana's governance and organizational links to emergency communications in the state are depicted in Figure 2.

Figure 2: Indiana's Governance and Organizational Links to Emergency Communications



Governance goals and objectives include the following:

Governance	
Goals	**Objectives**
1. The IPSC will develop an emergency communications model and leadership across the emergency communications ecosystem	1.1 The SIEC will establish a working group to review and revise the SIEC charter through the IPSC approval to address gaps in membership, responsibilities of system operators, and working groups
	1.2 The SIEC will establish technology working groups comprised of volunteers to address identified gaps
	1.3 The SIEC will create a standard template of programming for the various emergency communication systems and partners statewide, including the IPSC system

TECHNOLOGY AND CYBERSECURITY

Land Mobile Radio

IPSC manages and maintains SAFE-T, the statewide Project 25 (P25) Phase I 700/800 Megahertz (MHz) digital trunked voice and data system. The two zone core system includes over 191 tower sites and currently has over 105,000 subscriber radios serving local, state and federal first responders. User participation is voluntary and there are no service fees associated with using the system. Stakeholders have the ability to procure radio equipment from six authorized vendors to ensure cost competitiveness and more choice in products. There is an authorized subscriber equipment list, that is regularly updated, for the system found on their website.[4] Indiana is currently exploring plans to transition to SAFE-T Phase II in the coming years. Once funding is determined for Phase II, stakeholders will be informed of the transition timeline. This will allow users to plan and allocate funds for new subscriber units while gradually phasing out aging equipment as part of the life-cycle management process.

During Indiana's SCIP process, emergency communications stakeholders identified three challenges for the LMR environment:

- A need for telco redundancy at tower sites to improve system reliability
- Continuing education of first responders to ease system capacity overloads during large scale events
- Facilitating effective communication with mutual aid departments utilizing different systems
    - Currently eleven counties utilize and maintain separate P25 700/800 MHz radio systems, and nine counties use VHF radio as their primary communication
    - This patchwork of systems introduces further challenges for statewide programming standards, naming convention, and effective interoperability
    - However, all counties have access to the statewide system
        - Roughly 30 agencies use a long-term evolution (LTE) to LMR interface across multiple wireless vendors in combination with LMR

Technology goals in this SCIP have been developed to drive progress in the following LMR areas:

- All public safety radios are programmed with the IPSC recommended template, including counties with standalone systems who only use SAFE-T for interoperability purposes
- All public safety radios are capable of encryption as outlined in the State's encryption plan in order to be prepared for ongoing and future threats
- All public safety radios are capable of operating in a Time Division Multiple Access (TDMA) environment
- Ongoing education is provided to system users as changing technologies emerge
- SAFE-T is interoperable with neighboring State systems

[4] Integrated Public Safety Commission

911

The Indiana Statewide 911 Board provides a statewide private 911 network called IN911.[5] Through federal funding and the tireless work of many, all Indiana PSAPs have NG911-capable Call Processing Equipment (CPE), as of 2020.[6] The IN911 network is fully redundant at all levels, including transport to each PSAP, and all legacy local exchange carriers (LEC) network connections. The IN911 network is a fully private network making extensive use of internet protocol (IP) security protocols and procedures. In addition to these precautions, the network is monitored to automatically detect any operational abnormality.

The IN911 network is evolving to support more agencies and enhance public safety for Indiana residents and visitors. The Board has extended the IN911 network across state boundaries into Michigan, Ohio, and Kentucky to enable call transfers across state lines along with the location information associated with each call. Interconnectivity with Illinois is in progress.

Indiana has 118 PSAPs operating within the 92 counties of the state.[7] Two counties, Fountain and Warren, form a single combined 911 operating authority. Local 911 systems, established with one of the local exchange carriers, transports landline and Voice over Internet Protocol (VoIP) calls, and the IN911 network transports wireless 911 calls. County PSAPs are the primary answering points for wireless 911 calls, which may be transferred later to another PSAP for dispatch. In some instances, wireless 911 calls are routed directly to the PSAP serving the caller's location. These wireless routing profiles adhere to their legislative purpose, specifically for entities like colleges and Class II cities. The Indiana State Police (ISP) runs regional dispatch centers throughout the state as secondary PSAPs. ISP PSAP's are served by IN911's network.

The IN911 System uses a network of networks to form a secure Emergency Services Internet Protocol Network (ESInet) supporting a variety of public safety functions, including connections to the National Crime Information Center/Indiana Data and Communications, the Automated Fingerprint Identification System, and Criminal Justice Information Services.[8] All 92 counties in Indiana are connected to the ESInet and use Text-to-911.

Message EVOlution (MEVO) is a disaster recovery system provided to any PSAP in Indiana.[9] The MEVO system provides a backup 911 call delivery method if a PSAP needs to be evacuated or if the primary 911 equipment fails. All PSAPs have backup stationary phones; however, not all counties have deployable backup devices.

In 2022, IPSC launched an initiative called Project Gold Line to support over 100 emergency communication centers in Indiana.[10] One goal of this project is to introduce new FirstNet technology into 911 operations. Another goal of Project Gold Line is to prepare 911 staff to be more involved in their communications unit during disaster response.

[5] Indiana Statewide 911 Plan, 2020
[6] The History and Accomplishments of 911 In Indiana, 2020
[7] IN911 - Public Safety Answering Points
[8] IN911 - Text for 911 Platform
[9] IN911: MEVO
[10] FirstNet Authority

The SCIP process identified the need for improved and mandatory dispatcher training, enhanced backups, redundancy for their 911 system, and fiber last-mile connectivity at certain sites. Staffing shortages, pay issues, and difficulties in obtaining GIS data for NG911, which is sometimes managed by different agencies, were listed as significant concerns.

Emerging issues identified through the SCIP process include the 911 Board's funding for minimum training standards, which is utilized by 90 of 92 counties, and Indiana's implementation of additional system backups through MEVO INdigital vendor phones. The transition to cloud-based technology is ongoing for IN911, and there are legislative recommendations for geographic-based dispatch that cross jurisdictional boundaries.

Key areas of focus for 911 include:

- Continue expansion of location-based routing through the alignment of local GIS data.
- Achieve full adoption of i3 standards across all 118 PSAPs with their supporting vendors.
- Enhance education on NENA standards for GIS and master street address guide (MSAG) matching and location verification for the state's PSAPs.

Broadband

Indiana opted into FirstNet in 2017 and continues to expand its capabilities by building FirstNet cell sites and enhancing nearly 700 existing sites. Indiana will continue to enhance its statewide public safety broadband capabilities and usage through partnerships with FirstNet and other carriers to provide information regarding coverage gaps and concerns when the need arises.

In January 2020, IPSC implemented Motorola's Critical Connect, a P25 Inter-Sub System Interface (ISSI) gateway to allow IPSC the ability to integrate and link other P25 systems, as well as LTE-based solutions with the SAFE-T statewide P25 radio system. Implementation of Critical Connect allowed IPSC to integrate with other local and state P25 systems, as well as LTE-based solutions, such as AT&T ePush-to-Talk (ePTT), FirstNet Rapid Response, Verizon Push to Talk+, and other options.

Challenges discussed during the SCIP process include the integration and funding of LMR to LTE solutions. The state collaborates with the LMR to LTE providers to allow enhanced coverage and capacity for agencies for areas with LMR coverage gaps. Risks include an everchanging LTE communications landscape as technologies evolve.

Alerts and Warnings

In Indiana, there are 37 FEMA Integrated Public Alert and Warning System (IPAWS) alerting authorities.[11] Across the state, agencies use multiple different alerts and warnings applications and vendors. IDHS governs and serves as the point of contact for IPAWS at the state level. There is a working group in the IPAWS community to help standardize translations of multilingual messages.

Challenges identified during the SCIP process include:

- The need to update IPAWS alerting authorities' points of contact

[11] Federal Emergency Management Agency

- Manage the costs associated with ever changing compatible alerting software
- Emerging issues such as;
    - Understanding the multilingual demographics within a community
    - Identifying technology and resources to meet those needs
        - While artificial intelligence (AI) may assist in formulating messages, it must not be allowed to replace human review and final approval to avoid missing multilingual language nuances
- Difficulty of accurately translating messages across various languages with correct content and context, which often leads to increased time delays in communication

Key areas of focus for Alerts and Warnings include:

- Assess IPAWS methods for enhancing multilingual messaging.
- Develop a plan to increase county usage of IPAWS.
- Increase awareness of IPAWS' Standardized Message Design Dashboard through IDHS and inform users about training opportunities.

Cybersecurity

The Indiana Cybersecurity Hub website hosts multiple resources for cybersecurity, including best practices, standards, and recommendations.[12] The website also houses the 2021 Indiana Cybersecurity Strategic Plan and their 2017-2021 Indiana State of Cyber Report.

In 2019, the Indiana Executive Council on Cybersecurity (IECC) created the Indiana Emergency Manager Cybersecurity Toolkit.[13] This toolkit is primarily for emergency managers who serve their local communities and is organized into four main sections:

- A survey to assist emergency managers in planning with partners they work with to develop emergency and continuity of operations plans.
- A cybersecurity incident response plan template.
- A training and exercise guide.
- Several additional resources to assist in navigating this new and pervasive threat.

The IECC recently created two new cybersecurity toolkits free of cost.[14] The first is Healthcare Cyber in a Box, designed to provide organizations with three levels of expert guidance; basic, intermediate, and mature; and involves 10 critical areas of cybersecurity. The second is the Cyber Insurance Toolkit, intended to help businesses and organizations understand what cyber liability insurance is, what it covers and why it has become an increasingly important part of a company's risk management strategy. Drawing on the knowledge and expertise of insurance professionals and members of the legal profession, the Toolkit features a wealth of information from trusted sources. It covers various aspects, including the types of questions to consider asking as part of an

[12] Indiana Cybersecurity Hub - Home
[13] Indiana Emergency Manager Cybersecurity Toolkit, 2019
[14] Indiana Cybersecurity Hub - Home

underwriting document and understanding how to implement reasonable security controls while exercising due diligence.

The Indiana Information Sharing and Analysis Center (IN-ISAC) was developed by Indiana and key partners to mitigate cybersecurity risks among state agencies through sharing of threat information and collaboration on strategies.[15] IN-ISAC provides real-time network monitoring, vulnerability identification, and threat warnings. It reduces overall cost of cybersecurity through centralization of resources, use of large-scale purchasing, improved prevention efforts, and faster containment of threats.

Each county manages its own cybersecurity, while the state offers enterprise cybersecurity solutions for state agencies and a secure email feature for local agencies. As Indiana integrates more systems and capabilities, the risk of cyber attacks that could disrupt radio services increases. Additionally, the IN911 Board conducted a statewide cybersecurity assessment for all PSAPs in 2023-2024.

Challenges identified during the SCIP process include the need for effective vendor management of public safety networks and concerns over-reliance on third-party vendors. Risks and threats brought forward include the necessity for agencies to be familiar with available cybersecurity resources and response procedures, the need for incident response plans that are regularly tested before breaches occur, and the awareness of the increased attack surface as interoperability through various vendors expands.

GOALS AND OBJECTIVES

Technology and cybersecurity goals and objectives include the following:

Technology and Cybersecurity	
Goals	**Objectives**
2. Improve lifecycle management of the systems and equipment that enable emergency responders and public safety officials to share information efficiently and securely	2.1 Increase the compliance of the IPSC's Encryption Policy and supporting documents with state, local, and federal partners
	2.2 In reference to 2.1, establish coordinated use of over the air rekeying (OTAR) as appropriate for efficient and effective encryption key management across selected radios
	2.3 Create appropriate memorandum of understandings (MOUs) for interstate interoperability
	2.4 Assess appropriate Time Division Multiple Access (TDMA)-compliant radios for the IPSC system as the state prepares for Phase II migration
	2.5 Continue expansion of location-based routing through alignment of local geographic information system (GIS) data, including adoption of the i3 standards across all vendors and 118 Public Safety Answering Points (PSAPs)
3. Improve effective coordination of available operable and	3.1 911 Board cultivates a relationship with the IN Broadband Office to ensure fiber is in the plans for all 911 centers

[15] Indiana Cybersecurity Hub: Indiana Information Sharing and Analysis Center

Goals	Objectives
interoperable public safety communications capabilities for incidents and planned events	3.2 The IPSC Single Point of Contact (SPOC) will request FirstNet to stage a Satellite Cell on Light Truck (SatCOLT in Indiana for increased coverage
	3.3 Expand awareness across Indiana of public safety broadband network extenders for in-building coverage enhancements and finding ways to use across vendors as geographically appropriate and technologically feasible
	3.4 Increase capabilities, awareness, and utilization of Information and Communications Technology (ICT) Branch resources.
4. Develop and update comprehensive emergency communications plans and procedures that address the evolution of risks, capabilities, and technologies across Indiana's emergency communications ecosystem	4.1 The SIEC creates an Alerts and Warnings Working Group
	4.2 The Alerts and Warnings Working Group will develop an accurate Integrated Public Alert and Warning System (IPAWS) alerting authority database
	4.3 The IPAWS alerting authority database will be validated by the monthly radio test attendance
	4.4 Provide Primary, Alternate, Contingency, Emergency (PACE) planning training and exercise opportunities
5. Strengthen the cybersecurity posture of Indiana's emergency communications systems	5.1 The 911 Board centralizes current activities to increase education materials for cybersecurity awareness to 911 centers and other system owners across the state
	5.2 The SWIC Office will continue partnerships to provide cybersecurity education for local and state agencies

FUNDING

Indiana has a dedicated operating budget fund, provided by Indiana BMV certificate of title fees, that funds IPSC. IPSC currently receives a line-item appropriation for capital and preventive maintenance expenditures, but that funding is conditional and only available when the agency proves need. The 911 Board allocates its resources towards infrastructure management, while the only available grant for LMR funding—a homeland security grant focused on terrorism—is limited, highly competitive, and not primarily LMR-centric. Indiana's unique township governance structure adds complexity to public safety funding, often necessitating matching funds for volunteer equipment enhancements rather than full funding.

During the SCIP process it was noted that challenges faced include the need for local communities, particularly smaller and rural ones, to gain a better understanding of Indiana's grant processes and the deployment of limited funding for communications infrastructure. The cost of reliable and compatible radios and equipment, particularly for integration into the IPSC system, presents significant financial barriers, especially for rural communities. There are additional challenges regarding tower site capacity and the need for unfunded expansions, as well as funding mechanisms that have not evolved in 25 years, despite increasing costs.

The implementation of LMR to LTE integrations has also introduced new fiscal impacts for subscribers and agencies. IPSC does not charge end user/subscriber ongoing fees (i.e. monthly fees). The only expense to an agency to use the SAFE-T P25 system has been a one-time capital expenditure for the purchase of P25 radios. Agencies opting to integrate LMR to LTE into their communications plans have a new hurdle – ongoing monthly recurring subscription fees that the cellular carriers charge for LTE and PTT services.

Additionally, departments and agencies are struggling to secure the necessary funding for basic LMR equipment, potentially affecting interoperability within Indiana's public safety communications systems. As the technology evolves, particularly with the shift to TDMA models, the maintenance demands and associated costs for local radio systems are expected to rise.

Key areas of focus for Funding include:

- Secure funding for maintenance of ongoing cybersecurity measures for the LMR system.
- Identify alternative funding mechanisms or grants should be identified to replace the State Homeland Security Grant for radio replacement purposes.

Funding goals and objectives include the following:

Funding	
Goals	**Objectives**
6. Identify funding sources for achieving interoperable and public safety communication goals	6.1 The SIEC will develop a Funding Working Group with a minimum of 10 members
	6.2 The Funding Working Group identifies funding best practices at the county and local level to service the changing environment
	6.3 The SWIC's Office will research and distribute funding opportunities to locals, supporting their lifecycle technological needs
	6.4 IPSC and SIEC facilitates information on the importance of lifecycle funding best practices, especially for volunteer first responders
	6.5 The IPSC 6-year plan for transitioning to TDMA, as part of IPSC's lifecycle plan, has statewide support and a firm funding stream is established

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[16] of technical assistance (TA) available to assist with the implementation of the SCIP. TA requests are to be coordinated through the SWIC.

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

Goals	Objectives	Owners	Completion Dates
1. The Integrated Public Safety Commission (IPSC) will develop an emergency communications model and leadership across the emergency communications ecosystem	1.1 The Statewide Interoperability Executive Committee (SIEC) will establish a working group to review and revise the SIEC charter through the IPSC approval to address gaps in membership, responsibilities of system operators, and working groups	SIEC	1.1 July 2025
	1.2 The SIEC will establish technology working groups comprised of volunteers to address identified gaps		1.2 December 2025
	1.3 The SIEC will create a standard template of programming for the various emergency communication systems and partners statewide, including the IPSC system		1.3 December 2026
2. Improve lifecycle management of the systems and equipment that enable emergency responders and public safety officials to share information efficiently and securely	2.1 Increase the compliance of the IPSC's Encryption Policy and supporting documents with state, local, and federal partners	2.1 IPSC	2.1 December 2027
	2.2 In reference to 2.1, establish coordinated use of over the air rekeying (OTAR) as appropriate for efficient and effective encryption key management across selected radios	2.2 IPSC	2.2 December 2027
	2.3 Create appropriate memorandum of understandings (MOUs) for interstate interoperability	2.3 SWIC's Office	2.3 Ongoing
	2.4 Assess appropriate Time Division Multiple Access (TDMA)-compliant radios for the IPSC system as the state prepares for Phase II migration	2.4 IPSC	2.4 December 2027
	2.5 Continue expansion of location-based routing through alignment of local geographic information system (GIS) data, including adoption of the i3 standards across all vendors and 118 Public Safety Answering Points (PSAPs)	2.5 911 Board	2.5 Ongoing

[16] Emergency Communications Technical Assistance Planning Guide

Goals	Objectives	Owners	Completion Dates
3. Improve effective coordination of available operable and interoperable public safety communications capabilities for incidents and planned events	3.1 The 911 Board cultivates a relationship with the IN Broadband Office to ensure fiber is in the plans for all 911 centers	3.1 911 Board, Indiana Broadband Office	3.1 December 2026
	3.2 The IPSC Single Point of Contact (SPOC) will request FirstNet to stage a SatCOLT in Indiana for increased coverage	3.2 IPSC, SPOC	3.2 December 2024
	3.3 Expand awareness across Indiana of public safety broadband network extenders for in-building coverage enhancements and finding ways to use across vendors as geographically appropriate and technologically feasible	3.3 SIEC, IPSC	3.3 December 2026
	3.4 Increase capabilities, awareness, and utilization of Information and Communications Technology (ICT) Branch resources.	3.4 IPSC, IDHS	3.4 Ongoing
4. Develop and update comprehensive emergency communications plans and procedures that address the evolution of risks, capabilities, and technologies across Indiana's emergency communications ecosystem	4.1 The SIEC creates an Alerts and Warnings Working Group	4.1 SIEC	4.1 July 2025
	4.2 The Alerts and Warnings Working Group will develop an accurate Integrated Public Alert and Warning System (IPAWS) alerting authority database	4.2 SIEC Alerts and Warnings Working Group, IDHS	4.2 December 2025
	4.3 The IPAWS alerting authority database will be validated by the monthly radio test attendance	4.3 SIEC Alerts and Warnings Working Group, IDHS	4.3 Ongoing
	4.4 Provide Primary, Alternate, Contingency, Emergency (PACE) planning training and exercise opportunities	4.4 IPSC, IDHS	4.4 Ongoing
5. Strengthen the cybersecurity posture of Indiana's emergency communications systems	5.1 The 911 Board centralizes current activities to increase education materials for cybersecurity awareness to 911 centers and other system owners across the state	5.1 911 Board	5.1 December 2025
	5.2 The SWIC Office will continue partnerships to provide cybersecurity education for local's	5.2 SWIC's Office	5.2 December 2026
6. Identify funding sources for achieving interoperable and public safety communication goals	6.1 The SIEC will develop a Funding Working Group with a minimum of 10 members	6.1 SIEC	6.1 August 2024
	6.2 The Funding Working Group identifies funding best practices at the county and local level to service the changing environment	6.2 SIEC Funding Working Group	6.2 Ongoing
	6.3 The SWIC's Office will research and distribute funding opportunities to locals, supporting their lifecycle technological needs	6.3 SWIC	6.3 Ongoing

Goals	Objectives	Owners	Completion Dates
	6.4 IPSC and SIEC facilitates information on the importance of lifecycle funding best practices, especially for volunteer first responders	6.4 IPSC, SIEC	6.4 Ongoing
	6.5 The IPSC 6-year plan for transitioning to TDMA, as part of IPSC's lifecycle plan, has statewide support and a firm funding stream is established	6.5 IPSC	6.5 December 2027

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 Indiana's assessment of their progress against the markers as of 09/04/2024.

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
AI	Artificial Intelligence
AUXCOMM/AUXC	Auxiliary Emergency Communications
A&W	Alerts and Warnings
CAD	Computer-Aided Dispatch
CASM	Communication Assets Survey and Mapping
CISA	Cybersecurity and Infrastructure Security Agency
COML	Communications Unit Leader
COMT	Communications Unit Technician
COMU	Communications Unit Program
COOP	Continuity of Operations Plan
CPE	Call Processing Equipment
DHS	Department of Homeland Security
EPTT	Enhanced Push-to-Talk
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
IECC	Indiana Executive Council on Cybersecurity
IDHS	Indiana Department of Homeland Security
IN-ISAC	Indiana Information Sharing and Analysis Center
INCM	Incident Communications Center Manager
INTD	Incident Tactical Dispatcher
IP	Internet Protocol
IPAWS	Integrated Public Alert and Warning System
IPSC	Integrated Public Safety Commission
ISP	Indiana State Police
ISSI	Inter Radio Frequency Subsystem Interface
ITSL	Information Technology Service Unit Leader
LEC	Local Exchange Carriers
LMR	Land Mobile Radio
LTE	Long-Term Evolution
MEVO	Message EVOlution
MHz	Megahertz
MOU	Memorandum of Understanding

Acronym	Definition
NCSWIC	National Council of Statewide Interoperability Coordinators
NECP	National Emergency Communications Plan
NG911	Next Generation 911
OTAR	Over the Air Rekeying
P25	Project 25
PACE	Primary, Alternate, Contingency, Emergency
PSAP	Public Safety Answering Point
RADO	Radio Operator
RMS	Records Management System
SAAS	Software as a Service
SCIP	Statewide Communication Interoperability Plan
SIEC	Statewide Interoperability Executive Committee
SOP	Standard Operating Procedure
SPOC	Single 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
VoIP	Voice over Internet Protocol
WPS	Wireless Priority Service