CISA | CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

Louisiana Statewide Interoperability Executive Committee (SIEC)

October 23, 2019

Jim Lundsted, Central Sector Coordinator
Emergency Communications Division

CISA
CYBER+INFRASTRUCTURE

CISA Overview

Cybersecurity And Infrastructure Security Agency (CISA)			
Emergency Communications Division Enhances public safety interoperable communications at all levels of government, providing training, coordination, tools and guidance to help develop emergency communications	**Infrastructure Security Division** Provides strategic guidance to public and private partners, promotes a national unity of effort, and coordinates Federal efforts to promote the security and resilience of the Nation's critical infrastructure	**Cybersecurity Division** Offers cybersecurity programs and services to improve cybersecurity postures, including training, and technical assistance.	**Integrated Operation Division** Provides tools and training to partners to help partners in government and industry manage the risks to their assets, systems, and networks.
Stakeholder Engagement Division	Leverages partnerships to build capacity for resilience across the Nation's critical infrastructure and the cybersecurity community.		
National Risk Management Center	A planning, analysis, and collaboration center that identifies and addresses the most significant risks to the Nation's critical infrastructure		

- Created by the *Cybersecurity and Infrastructure Security Agency Act of 2018*

- Leads the Federal Government's cyber security, critical infrastructure protection, and emergency communications efforts

- Unites efforts from across government and industry to understand and manage risks together

CISA
CYBER+INFRASTRUCTURE

2

What ECD Does

Core Competencies

National and Statewide Planning & Execution
Develop and implement nationwide emergency communications policy and plans, including the National Emergency Communications Plan (NECP) and 56 Statewide Communications Interoperability Plans (SCIPs)

Federal Grant Coordination
Manage funding, sustainment, and grant programs to support communications interoperability

National Governance
Support nationwide sharing of best practices and lessons learned through facilitation of the SAFECOM and Emergency Communications Preparedness Center (ECPC) governance bodies

Priority Telecommunications Services (PTS)
Provide PTS over commercial networks to enable national security and emergency preparedness personnel to communicate during congestion scenarios across the nation

Technical Assistance & Outreach
Build capacity with Federal, State, Local, Tribal, and Territorial stakeholders by providing technical assistance, training, resources, and guidance

Assessment and Reports
Assess the Nation's progress regarding interoperable emergency communications to identify remaining gaps

CISA
CYBER+INFRASTRUCTURE

3

The SAFECOM Interoperability Continuum

|	Limited Leadership, Planning, and Collaboration Among Areas with Minimal Investment in the Sustainability of Systems and Documentation					High Degree of Leadership, Planning, and Collaboration Among Areas with Commitment to and Investment in Sustainability of Systems and Documentation
Governance		Individual Agencies Working Independently	Informal Coordination Between Agencies	Key Multi-Discipline Staff Collaboration on a Regular Basis	Regional Committee Working within a Statewide Communications Interoperability Plan Framework	
Standard Operating Procedures		Individual Agency SOPs	Joint SOPs for Planned Events	Joint SOPs for Emergencies	Regional Set of Communications SOPs	National Incident Management System Integrated SOPs	
Technology	DATA ELEMENTS: Swap Files / VOICE ELEMENTS: Swap Radios	Common Applications / Gateway	Custom-Interfaced Applications / Shared Channels	One-Way Standards-Based Sharing / Proprietary Shared System	Two-Way Standards-Based Sharing / Standards-Based Shared System	
Training & Exercises		General Orientation on Equipment and Applications	Single Agency Tabletop Exercises for Key Field and Support Staff	Multi-Agency Tabletop Exercises for Key Field and Support Staff	Multi-Agency Full Functional Exercises Involving All Staff	Regular Comprehensive Regionwide Training and Exercises	
Usage		Planned Events	Localized Emergency Incidents	Regional Incident Management	Daily Use Throughout Region	

4

National Emergency Communications Plan

The NECP was released September 25, 2019.
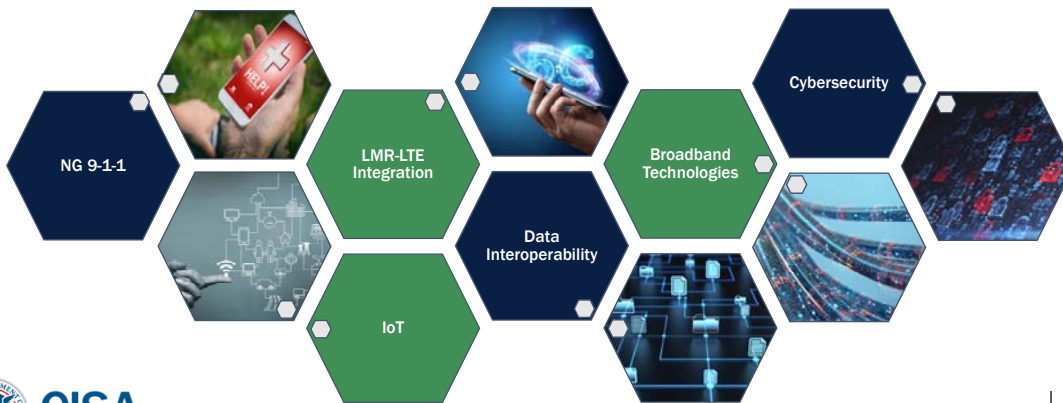
The NECP is available for download at:
www.cisa.gov/necp

For more information on the NECP, contact:
necp@cisa.dhs.gov

National Emergency
Communications Plan

September 2019

CISA

CISA
CYBER+INFRASTRUCTURE

5
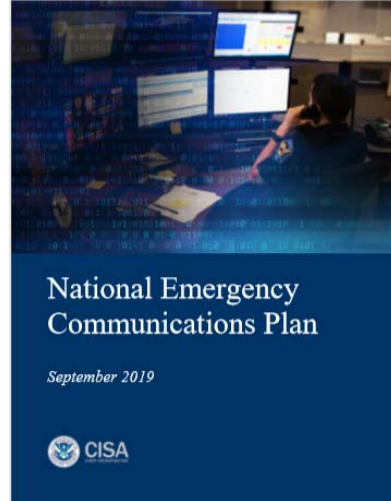
Drivers of Change

Since the NECP's first publication in 2008 and its update in 2014, there have been significant advancements in technology and changes to the emergency communications landscape, affecting the Nation's ability to communicate. While, new technologies have increased capabilities, they also introduce new challenges around data interoperability and cybersecurity. Examples of drivers of change include:

- NG 9-1-1
- LMR-LTE Integration
- Cybersecurity
- Broadband Technologies
- Data Interoperability
- IoT

CISA
CYBER+INFRASTRUCTURE

6

The Updated NECP

Several of the key updates to the NECP include, but are not limited to:

A Focus on Adaptive Governance Strategies

Embracing adaptive governance models that are flexible and support collaborative decision-making and expand membership composition

Advocacy for Updated Training & Exercise Programs

Expanding training and exercise participation and content to improve operational policies and procedures

A Technology and Infrastructure Goal

Building upon the previous Research and Development Goal and expanding to cover key data interoperability, NG911, and FirstNet considerations

A Cybersecurity Goal

Taking proactive measures to manage cybersecurity risks and strengthen the cyber posture of the Emergency Communications Ecosystem

Expanded Concept of Communications Resiliency

Expanded to include periodic testing and user-usage observations, active resources sharing, and regionalization of shared infrastructure, networks, and services

Recommendations for Enhanced Communication Coordination

Establishing and maintaining a repeatable process to periodically observe and record user proficiency for communications systems

CISA CYBER+INFRASTRUCTURE

7

Emergency Communications Iceberg Graphic

The True Cost and Scope of Emergency Communications

What Most People See

911
- Voice Systems (Telephone)
- Computer Aided Dispatch (CAD) Systems
- Transition to Next Generation 911 (NG911)

What People Don't See

Radio Communications Systems
- Mobile and Portable Land Mobile Radio (LMR)
- Interoperability Maintenance Costs
- Communication Towers
- Tower Equipment Sheds

Broadband & Data Systems
- Mobile Data Terminals (MDT)
- FirstNet
- Government Emergency Telecommunications Service (GETS)
- Wireless Priority Service (WPS)

Alerts & Warnings
- Outdoor Warning Systems
- Emergency Alert System (EAS)
- Wireless Emergency Alerts (WEA)
- IPAWS (including silver/amber alerts)
- TV/Radio/Website/Media Updates
- Social Media Outlets

Governance
- SWIC / Communications Champion
- Statewide Communications Office
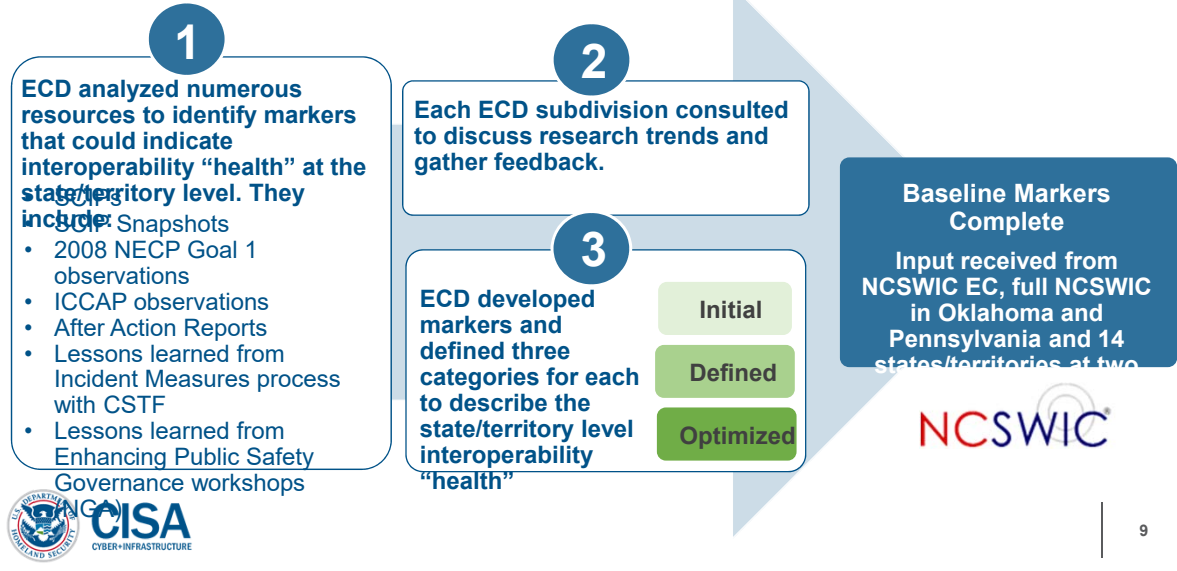- Strategic Planning

Training & Exercises
- Telecommunicator/Dispatch Training and Retention
- Agency LMR, Telephone, Alerts/Warning procedures
- Agency System Maintenance staff (technicians, engineers)
- Incident Communications Training
- Communications Exercise (tabletop, functional)
- Technical Emergency Response Training (TERT)
- Incident Communications Unit staff training, including:
  – Communications Unit Leader (COML)
  – Communications Technician (COMT)
  – Incident Tactical Dispatcher (INTD) Training
  – Radio Operator (RADO) Training
  – Information Technology Service Unit Leader (ITSL)
  – Audio Gateway Information and Training
  – Cybersecurity Training and Awareness

Cybersecurity
- Expertise and Planning
- Tools and Solutions
- Risk and Vulnerability Management
- Prevention Equipment and Training

CISA CYBER+INFRASTRUCTURE

State Interoperability Marker Development

1

ECD analyzed numerous resources to identify markers that could indicate interoperability "health" at the state/territory level. They include:
- SCIP Snapshots
- 2008 NECP Goal 1 observations
- ICCAP observations
- After Action Reports
- Lessons learned from Incident Measures process with CSTF
- Lessons learned from Enhancing Public Safety Governance workshops (NGA)

2

Each ECD subdivision consulted to discuss research trends and gather feedback.

3

ECD developed markers and defined three categories for each to describe the state/territory level interoperability "health"

Initial

Defined

Optimized

Baseline Markers Complete

Input received from NCSWIC EC, full NCSWIC in Oklahoma and Pennsylvania and 14 states/territories at two

NCSWIC

9

Benefits for States and Territories

Understand impacts of interoperability efforts

Improve coordination and buy-in from lawmakers and executive branch staff

Reduce workload and reporting requests by eliminating SCIP Snapshots and reducing time required to gather data

Improve strategic planning and implementation aligned to ecosystem

Justify grant funding and state budget requests

Enhance the SCIP planning process

Improve coordination with locals

Enhance governance body participation and membership

10

Benefits for CISA

Understand state/territory interoperability capabilities and gaps and assist in improving the SCIP process

Improve alignment to the NECP

Improve TA offerings to better meet state/territory needs

Justify resource requirements to DHS leadership, OMB, Congress, and the President

Respond to Congressional, GAO and OMB requests for ECD program impacts

CISA CYBER+INFRASTRUCTURE

11

DATA CAPTURE PROCESS

Governance

Marker #	Best Practices / Performance Markers	Initial	Defined	Optimized
1	▪ State-level governing body established (e.g., SIEC, SIGB) ▪ Governance framework 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 executive order	Governing body role established through 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

▪ **Objective:** Complete governance lane in group setting and continue in breakouts
▪ **Outcome:** Complete submission of State Interoperability Markers data

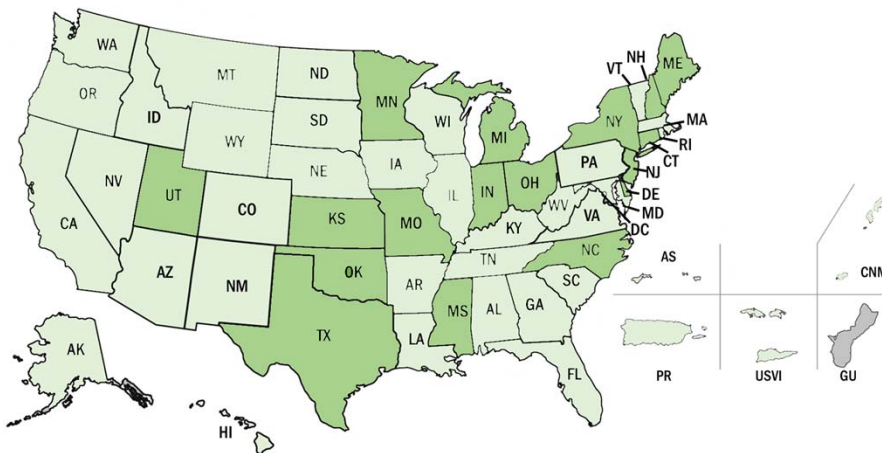**CISA** CYBER+INFRASTRUCTURE

12

National Completion Map
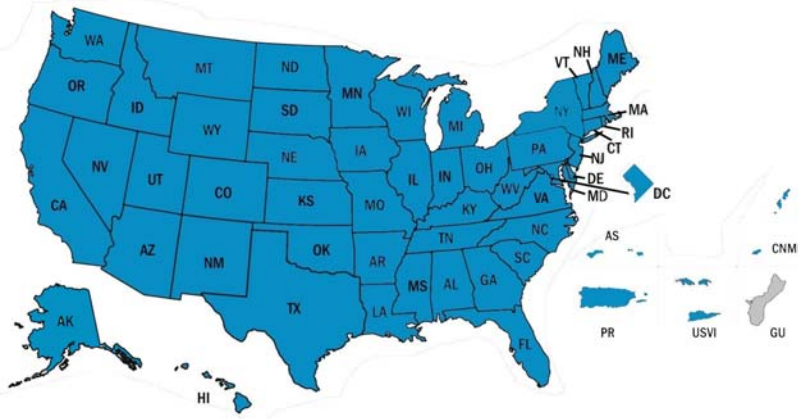
Key

States / Territories with State Marker Data

States / Territories without State Marker Data

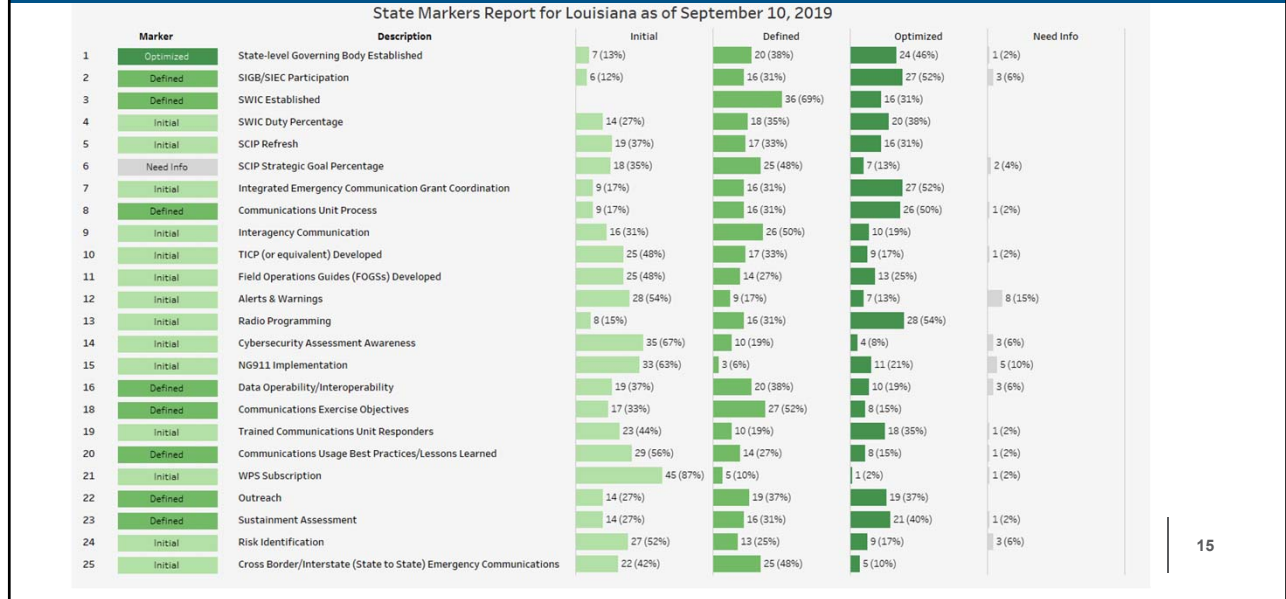* 55 States and territories have now completed and submitted their markers

13

State Marker Status Map

Overall State Averages

- 0% - Optimized
- 34% - Defined
- 64% - Initial
- 2% Incomplete

14

Preliminary Louisiana Self-Assessment

State Markers Report for Louisiana as of September 10, 2019

#	Marker	Description	Initial	Defined	Optimized	Need Info
1	Optimized	State-level Governing Body Established	7 (13%)	20 (38%)	24 (46%)	1 (2%)
2	Defined	SIGB/SIEC Participation	6 (12%)	16 (31%)	27 (52%)	3 (6%)
3	Defined	SWIC Established		36 (69%)	16 (31%)	
4	Initial	SWIC Duty Percentage	14 (27%)	18 (35%)	20 (38%)	
5	Initial	SCIP Refresh	19 (37%)	17 (33%)	16 (31%)	
6	Need Info	SCIP Strategic Goal Percentage	18 (35%)	25 (48%)	7 (13%)	2 (4%)
7	Initial	Integrated Emergency Communication Grant Coordination	9 (17%)	16 (31%)	27 (52%)	
8	Defined	Communications Unit Process	9 (17%)	16 (31%)	26 (50%)	1 (2%)
9	Initial	Interagency Communication	16 (31%)	26 (50%)	10 (19%)	
10	Initial	TICP (or equivalent) Developed	25 (48%)	17 (33%)	9 (17%)	1 (2%)
11	Initial	Field Operations Guides (FOGSs) Developed	25 (48%)	14 (27%)	13 (25%)	
12	Initial	Alerts & Warnings	28 (54%)	9 (17%)	7 (13%)	8 (15%)
13	Initial	Radio Programming	8 (15%)	16 (31%)	28 (54%)	
14	Initial	Cybersecurity Assessment Awareness	35 (67%)	10 (19%)	4 (8%)	3 (6%)
15	Initial	NG911 Implementation	33 (63%)	3 (6%)	11 (21%)	5 (10%)
16	Defined	Data Operability/Interoperability	19 (37%)	20 (38%)	10 (19%)	3 (6%)
18	Defined	Communications Exercise Objectives	17 (33%)	27 (52%)	8 (15%)	
19	Initial	Trained Communications Unit Responders	23 (44%)	10 (19%)	18 (35%)	1 (2%)
20	Defined	Communications Usage Best Practices/Lessons Learned	29 (56%)	14 (27%)	8 (15%)	1 (2%)
21	Initial	WPS Subscription	45 (87%)	5 (10%)	1 (2%)	1 (2%)
22	Defined	Outreach	14 (27%)	19 (37%)	19 (37%)	
23	Defined	Sustainment Assessment	14 (27%)	16 (31%)	21 (40%)	1 (2%)
24	Initial	Risk Identification	27 (52%)	13 (25%)	9 (17%)	3 (6%)
25	Initial	Cross Border/Interstate (State to State) Emergency Communications	22 (42%)	25 (48%)	5 (10%)	

15

# Future SIEC Membership Feedback

- At a future SIEC meeting, ECD would like to conduct a brief review and validation of your interoperability markers

- Using live capture and an anonymous polling tool called "Poll Anywhere" we can quickly validate your baseline

- State interoperability markers will drive our efforts in future ICTAP Technical Assistance program offerings, Statewide Communications Interoperability Plan (SCIP) workshops, and implementation of *National Emergency Communications Plan* (NECP) goals

CISA
CYBER+INFRASTRUCTURE

16

FY2020 ICTAP Technical Assistance

- ECD's Interoperable Communications Technical Assistance Catalog will be available soon

- Requests are coordinated through your Statewide Interoperability Coordinator (SWIC)

- https://www.dhs.gov/publication/ictapscip-resources
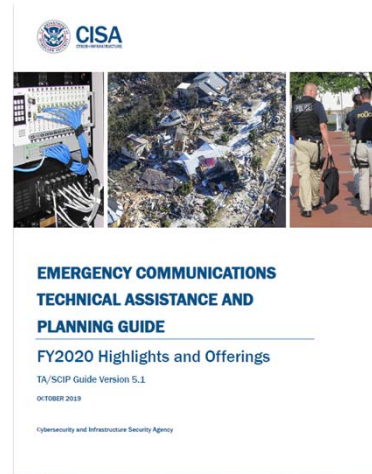
17

Questions?

18

Contact

Cybersecurity and Infrastructure Security Agency
Emergency Communications Division
https://www.cisa.gov/emergency-communications

Jim Lundsted
Central Sector Coordinator – Regions 6 & 7
Office: 573-298-0484 Mobile: 202-630-1177
James.Lundsted@hq.dhs.gov

CISA
CYBER+INFRASTRUCTURE

19

Backup Slides

Backup Slides

CISA
CYBER+INFRASTRUCTURE

How WPS Works

How WPS "Really" Works