IMPLEMENTING THE NECP WEBINARS

IS THIS THING ON?
USING BACKUP COMMUNICATIONS SYSTEMS TO ENSURE MISSION READINESS

APRIL 26, 2023

Agenda

- National Emergency Communications Plan (NECP) and SAFECOM Nationwide Survey (SNS): Testing Backup Systems
- Speaker Presentation
- Resources and Actions
- Question and Answer Session

Speakers

Charlee Hess
Cybersecurity and Infrastructure Security Agency

Charles Bryson
FCC Region 20 Planning Committee Chair

National Regional Planning Council (NRPC) Chair

Maryland FiRST statewide 700 MHz public safety communications radio system technical advisor

Delaware statewide 700 MHz system advisor

Public safety project consultant (for various states)

National Emergency Communications Plan

NECP Vision

To enable the Nation's emergency response community to communicate and share information securely across communications technologies in real time, including all levels of government, jurisdictions, disciplines, organizations, and citizens impacted by any threats or hazards event

National Emergency Communications Plan

Mandate
The NECP is mandated by Title XVIII of the Homeland Security Act of 2002 (as amended)

Guidance
Provides guidance for those who plan for, coordinate, invest in, and use communications

Stakeholders
Helps stakeholders update policies, governance, planning, and protocols

NECP Goals

Goal 1
Governance & Leadership

Goal 2
Planning & Procedures

Goal 3
Training, Exercises, & Evaluation

Goal 4
Communications Coordination

Goal 5
Technology & Infrastructure

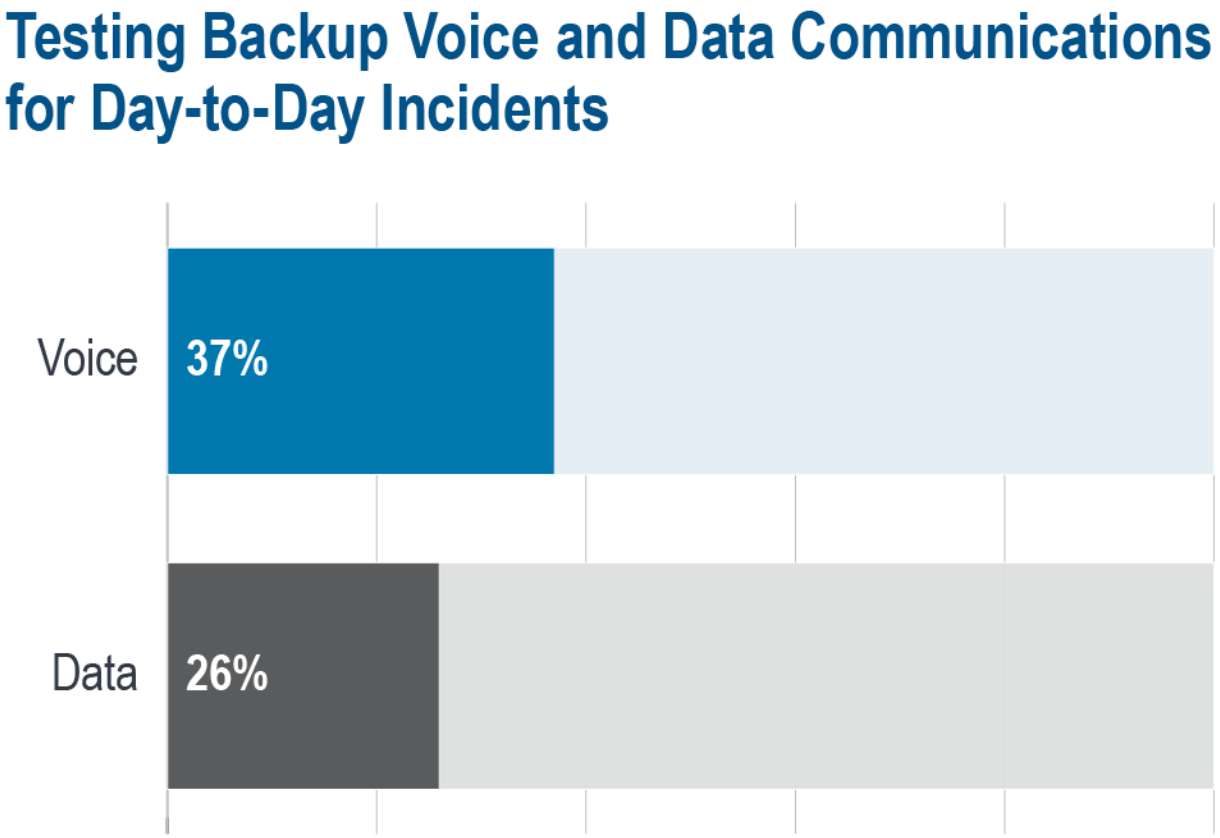
Goal 6
Cybersecurity

SAFECOM Nationwide Survey (SNS)

The 2018 SNS consisted of 38 questions that **span the 5 elements of the *SAFECOM Interoperability Continuum***, plus a **security element** that accounted for cybersecurity

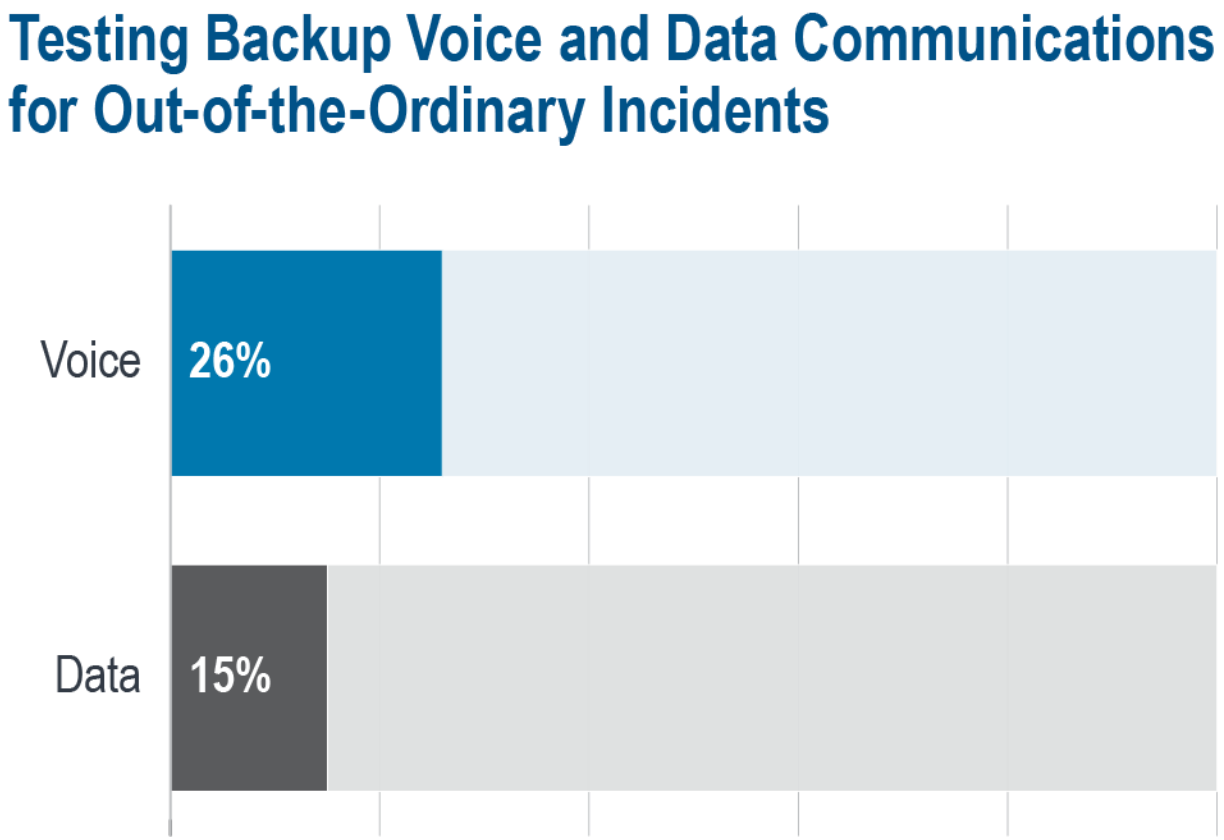
SNS: Testing Backup Systems for Day-to-Day Incidents

For day-to-day incidents, **37%** of public safety organizations test **backup voice** communications and **26%** test **backup data** communications



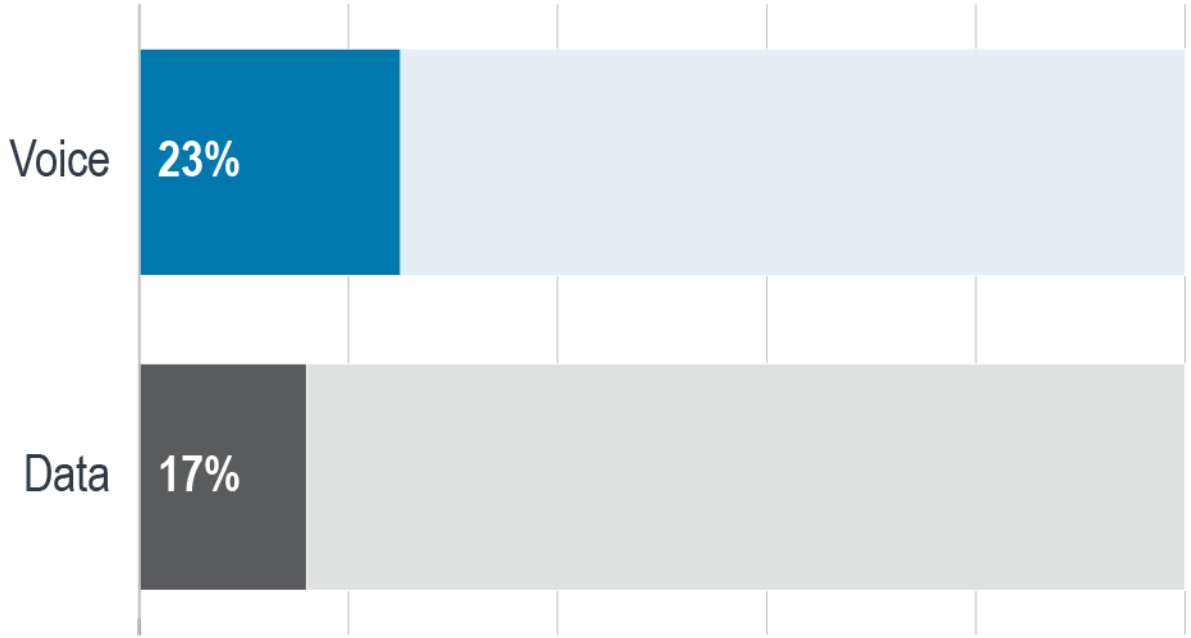
SNS: Testing Backup Systems for Out-of-the-Ordinary Incidents

For out-of-the ordinary situations when **backup systems** are **most likely to be needed**, just 26% of organizations test backup voice and only 15% test backup data



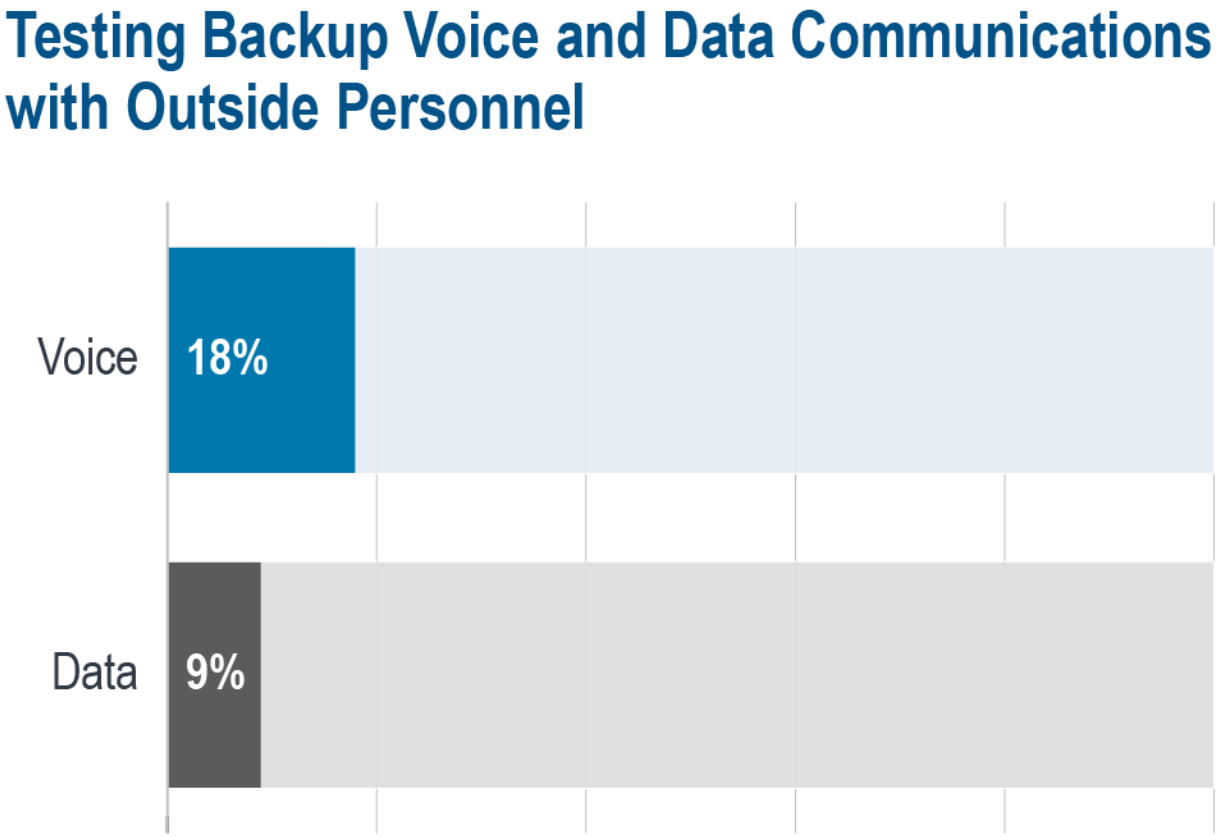
SNS: Testing of Backup Systems - SOPs

Testing Backup Voice and Data Communications According to SOPs



23% of public safety organizations test **backup voice** communications and only **17%** test **backup data** communications in accordance with SOPs

SNS: Testing Backup Systems - Outside Personnel



18% of public safety organizations test backup voice communications and only 9% of public safety organizations test backup data communications with **personnel beyond their organization**

NECP Goal 4: Communications Coordination

Strengthen resilience and continuity of communications throughout operations

Success Indicator 4.4.1: Public safety organizations establish sufficient testing and usage observations of all operable and interoperable primary, secondary, and backup communications systems

NECP Goal 4: Communications Coordination

Enhance coordination and effective usage of public safety communications resources at all levels of government

Success Indicator 4.2.1: Public safety organizations maintain and readily share comprehensive information about features, functionality, and capabilities of operable and interoperable communication resources

Additional Success Indicators

Goal 1
Governance & Leadership

- Adapt governance strategies to address communications capabilities and risks

Goal 2
Planning & Procedures

- Update plans to incorporate the acquisition, testing, and maintenance of backup communications systems

Goal 3
Training, Exercises, & Evaluation

- Ensure training for usage of backup systems during multi-agency response operations

Additional Success Indicators

Goal 5
Technology & Infrastructure

- Ensure backup communications systems meet mission-critical needs

Goal 6
Cybersecurity

- Mitigate cyber vulnerabilities for primary, secondary, and backup systems

Speaker Presentation

Charles Bryson

- FCC Region 20 Planning Committee Chair
- National Regional Planning Council (NRPC) Chair
- Maryland FiRST statewide 700 MHz public safety communications radio system technical advisor
- Delaware statewide 700 MHz system advisor
- Public safety project consultant (for various states)
- Retired Commonwealth of Virginia (police officer, university administrator, and adjunct faculty member at Virginia Commonwealth University and Reynolds Community College)

Infrastructure Backup for Communications Systems

Backup issues are complex and often, weak points in systems that are not known until they fail. Some examples include:

- Electricity, UPS systems can suffer transfer switch failures – lesson learned, sites may require added battery power as well as transfer switch redundancy
- Microwave dish mounting – When testing systems for acceptance, you can't produce high wind loads – redundancy may be provided by fiber optics of commercial broadband carriers
- Fiber optic cable cuts – Redundant communications paths are needed such as with Maryland FiRST, paths are engineered from end points to ensure that fiber is in separate modalities; e.g., different routes are used for fiber or microwave is the redundant means of transmission

Backup for Radio Frequency (RF) Systems

PACE Planning – Primary, Alternate, Contingency, and Emergency

- Primary is the day-to-day communications system of a public safety organization. What happens if it fails?
- Identify an alternate means of communications; e.g., another system that provides coverage for first responders
- If the primary and alternate both fail, what's the contingency? One contingent option could be to switch to a wireless broadband carrier with Push-to-Talk (PTT) functionality
- What's the final option available to maintain communications? This varies by jurisdiction and may range from very basic, e.g., first responders go to predetermined locations and use landline telephones, to use of other alternatives such as satellite phones

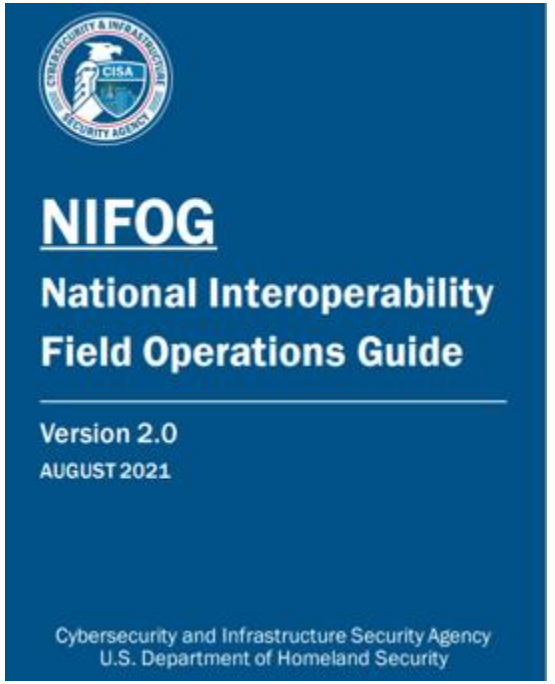
What is important is that organizations have a plan – it's tough to develop plans after the disaster has hit

Interoperability

- **Interoperability is very important, but the record on implementation is mixed**
- **Local routine use of interoperable communications is typically good because**
  1. Local leaders understand and support the need for interoperability
  2. First responders plan for interoperability and develop procedures
  3. There is training and feedback in “after action” reports
  4. On scene protocols define incident based operational leadership
  5. When there are technological failures, administrators act to resolve issues
- **All of this should sound familiar; the issues match the first five goals of the NECP**
- **Interoperability challenges**
  1. When unexpected events occur requiring extraordinary resources, interoperability can be extremely challenging; e.g., January 6, 2021 riot at the U.S. Capitol, weather disasters, and other catastrophic events

Interoperability Resources

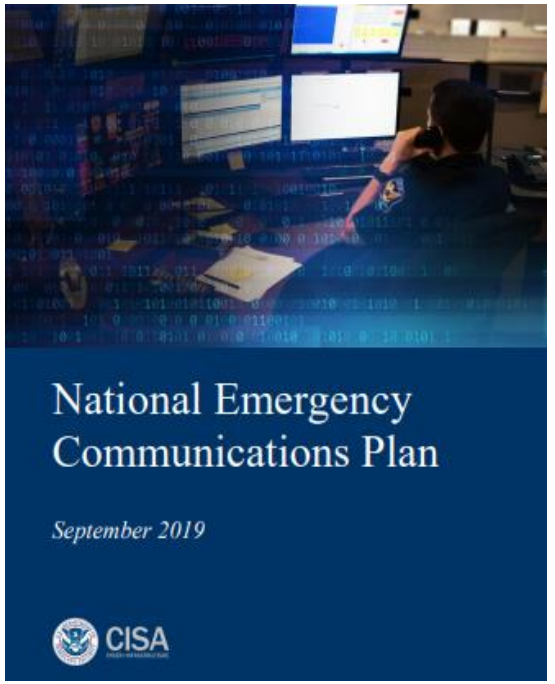
- 800 MHz nationwide interoperability channels 8CALL90 and 8TAC91-94
- 700 MHz nationwide interoperability channels (32 frequency pairs)
- Deployable trunking channels (six frequencies)
- Other resources as identified in the National Interoperability Field Operations Guide (NIFOG)
- Challenges to interoperability
  1. Devices that do not support **nationwide** standards such as Project 25 (P25) Phase 1 and 2 or Advanced Encryption Standard (AES)
  2. Devices not programmed to support all nationwide interoperability resources; e.g., 700 MHz interoperability channels
  3. Failure to plan or exercise interoperability



Interoperability Doesn't Happen Overnight

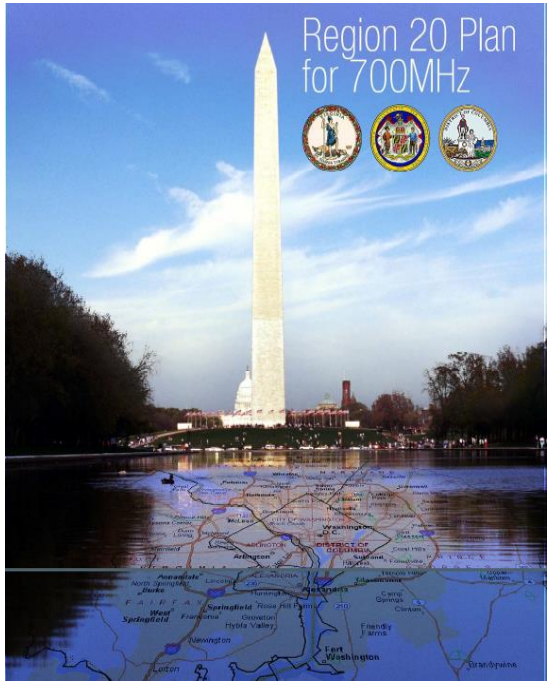
- **The roadmap to support true nationwide interoperability in anticipation of extraordinary events is tough as outlined in the NECP goals**

1. ***Leadership*** to recognize the importance of planning for events outside of one's normal operating areas
2. ***Planning*** moves from local to regional and multi-jurisdictional; e.g., FEMA regions
3. ***Training*** moves to regional and multi-jurisdictional
4. ***Coordination*** moves to levels where jurisdictions have to work with unfamiliar resources (COMM-L)
5. ***Technology/infrastructure*** needs to support many new first responders



Interoperability Leadership Challenges

- In multistate regions, it can be challenging to get administrators on the same interoperability page. Are there alternatives?
- Because Region 20 covers two states and the District of Columbia, we started the road to regional interoperability by working with the Statewide Interoperability Coordinators (SWIC) and representatives from the Metropolitan Washington Council of Governments (MWCOG)
- An interoperability template was developed that encompassed all of our nationwide interoperability resources as well as special planning for National Special Security Events (NSSE) in the nation's capital



Region 20 Interoperability Template

Was the template successful immediately? No for many reasons:

- The first version was essentially a beta and some departments did not want to flash their radios for a non-finalized version
    1. This was a legitimate concern as we learned many lessons during the 2021 presidential inauguration that took us back to the planning drawing board
- Some agencies reported a lack of real estate in devices to add the new zones
- There was also an issue of timing; radio flashes occur at certain times
- Current status: Many, but not all, challenges have been resolved and most MWCOG jurisdictions, as well as many state and local agencies will be using the template

Strengthening Interoperability in Region 20

The MWCOG is considering two grant proposals to:

- Add 700 MHz nationwide interoperability stations in DC and northern Virginia
- Fund expansion of the Maryland FiRST statewide public safety radio station into sites within DC and Arlington County, VA

These needs evolved following January 6, 2021 and the events at the U.S. Capitol

Takeaways and Recommendations

1. If localities have not developed plans for local interoperability, **START!** Plan for communications in the same frequency bands or develop procurement strategies for multiband devices
2. Work with SWICs and Regional Planning Committees to plan for the unexpected. SWICs need the support and cooperation of state and local governments
3. Strengthen interoperability by looking past local requirements for interoperable communications. Technologies such as Inter Radio Frequency Subsystem Interface (ISSI) and cloud-based interoperability systems should be evaluated
4. Plan for technological upgrades that meet ***national standards*** for P25 Phase 1 and 2 as well as AES encryption and multiband radios
5. Develop plans for testing and exercising interoperability

Resources

CISA Resources

- National Emergency Communications Plan
- National Council of Statewide Interoperability Coordinators (NCSWIC) Membership
- Auxiliary Emergency Communications Training Course
- Emergency Communications Systems Value Analysis Guide
- Emergency Communications System Life Cycle Planning Guide
- Shared Resources (Shares) High Frequency (HF) Radio Program
- Public Safety Communications Network Resiliency Self-Assessment Guidebook
- Statewide Communication Interoperability Plans Workshops
- Regional Interoperable Communications Plan (RICP) Template
- Priority Communications Services
- Interoperable Communications Technical Assistance Program Service Offerings Guide

Additional Resources

Federal Emergency Management Agency (FEMA) Resources

- National Incident Management System (NIMS)

Federal Communications Commission Resources

- Network Resiliency for Small and Rural Communications Providers

National Public Safety Telecommunications Council (NPSTC) Resources

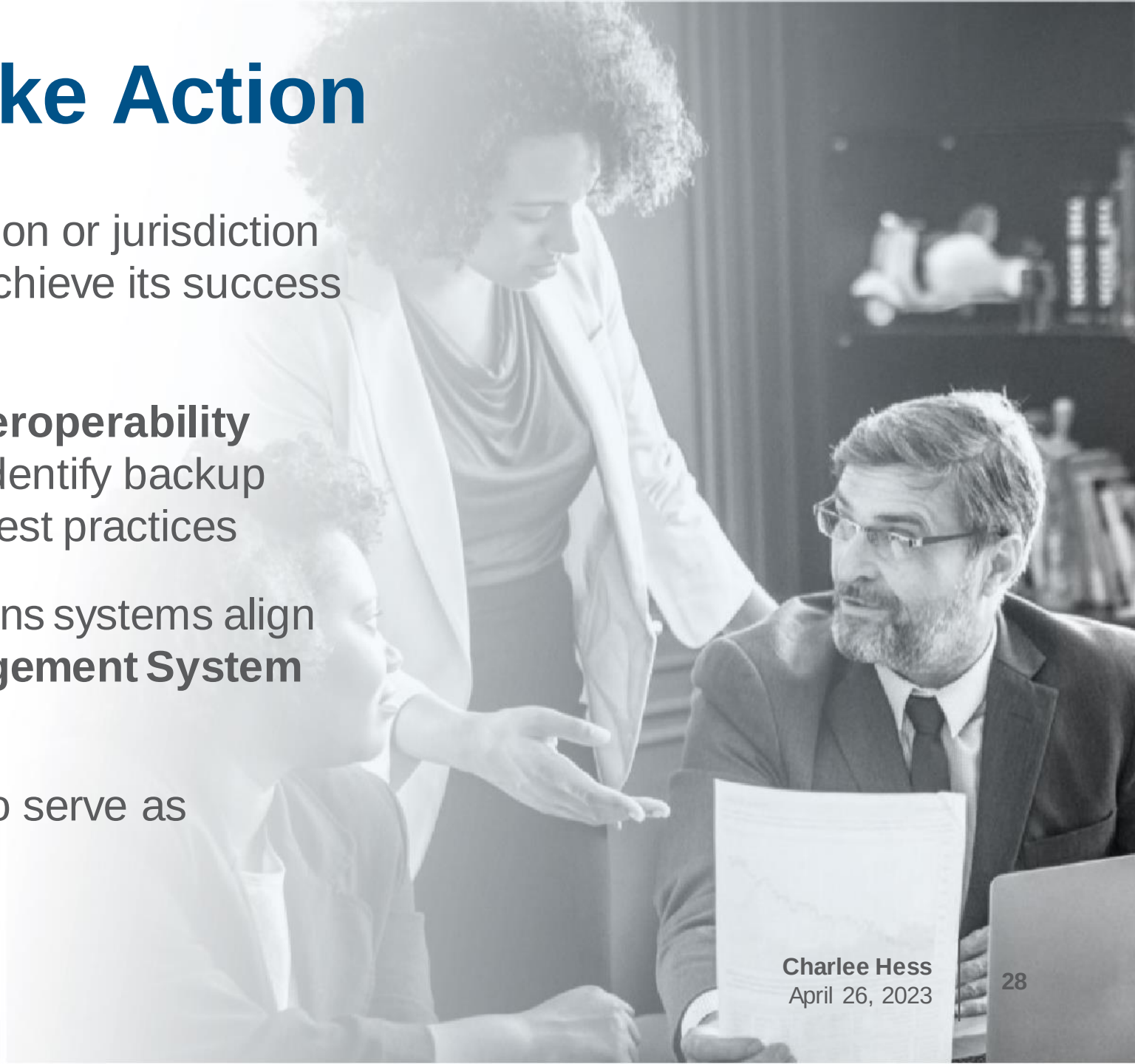
- Best Practices for Public Safety Interoperable Communications

SAFECOM Resources

- SAFECOM Nationwide Survey
- SAFECOM Interoperability Continuum

How You Can Take Action

- **Take steps** for your organization or jurisdiction to implement the NECP and achieve its success indicators
- **Leverage** your **Statewide Interoperability Coordinator (SWIC)** to help identify backup emergency communications best practices
- **Ensure** backup communications systems align with **National Incident Management System (NIMS)** principles
- **Optimize** existing resources to serve as deployable backup assets



Questions?

SAFECOM® NATIONWIDE SURVEY

COMING SOON

INFLUENCE THE FUTURE OF EMERGENCY COMMUNICATIONS

visit **cisa.gov/sns**
email **sns@cisa.dhs.gov**

Upcoming Webinars

Join the Cybersecurity and Infrastructure Security Agency for webinars focused on:

Implementing the National Emergency Communications Plan

Bookmark our webpage to check back for future webinars:
https://www.cisa.gov/necp-webinars

For more information on the NECP:

www.cisa.gov/necp

NECP@cisa.dhs.gov


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY