CISA | CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

IMPLEMENTING THE NECP WEBINARS

CYBER INCIDENT RESPONSE PLANNING FOR EMERGENCY COMMUNICATIONS

OCTOBER 26, 2022

Agenda

- National Emergency Communications Plan (NECP) and SAFECOM Nationwide Survey (SNS): Cybersecurity
- Cyber Incident Response Planning Panel Discussion
- Resources and Actions
- Question and Answer Session

Panelists

Charlee Hess
Cybersecurity and Infrastructure Security Agency

Charlie Guddemi
District of Columbia Homeland Security and Emergency Management Agency

Teddy Kavaleri
District of Columbia Office of Unified Communications

Karla Jurrens
Texas Department of Public Safety

Joseph Oregón
Cybersecurity and Infrastructure Security Agency, Region 9

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

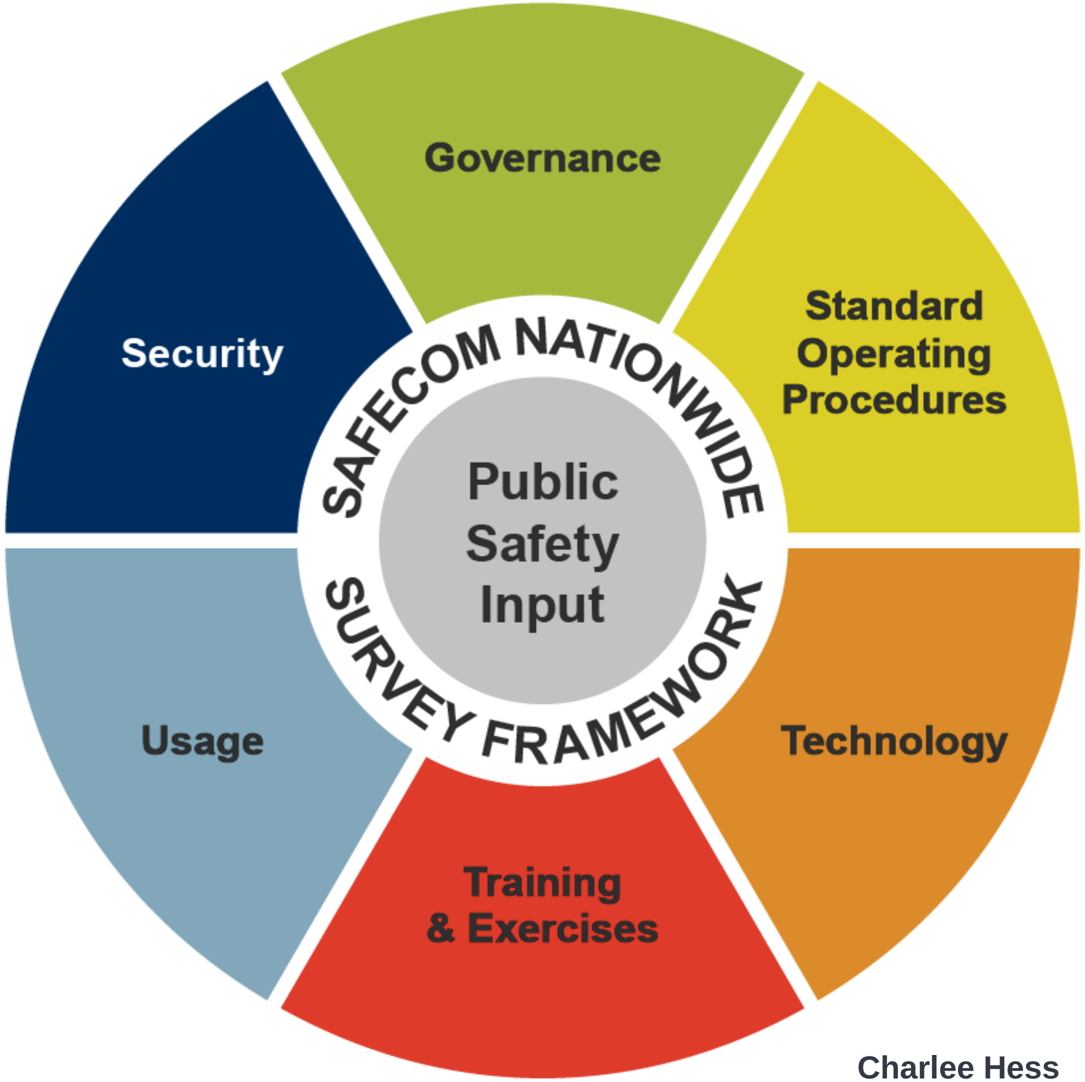
Goal 5
Technology & Infrastructure

Goal 6
Cybersecurity

Charlee Hess
October 26, 2022

SAFECOM Nationwide Survey (SNS)

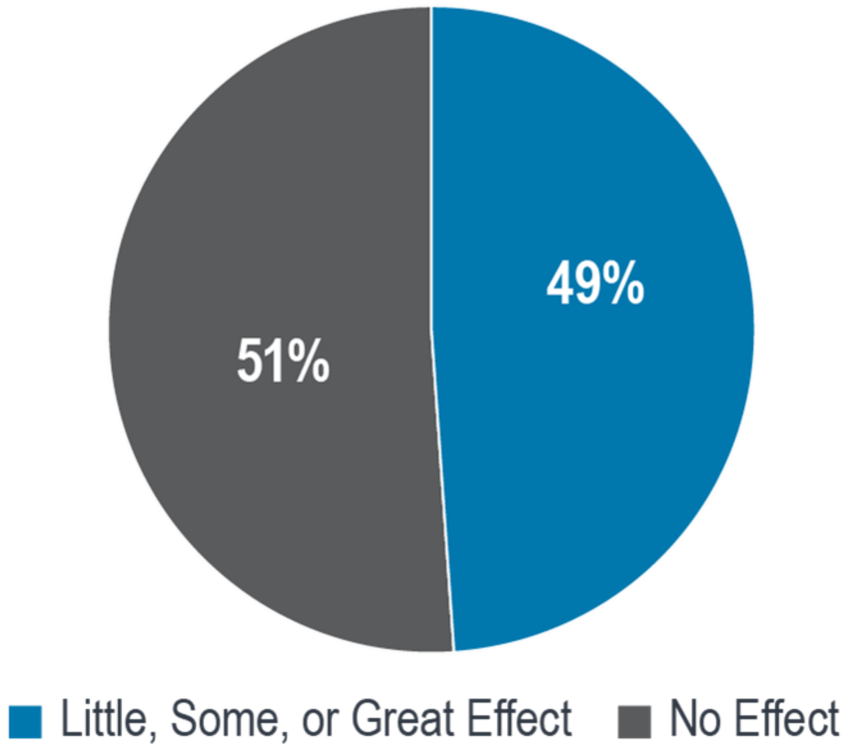
The 2018 SNS consisted of 38 questions that **span the 5 elements of the *SAFECOM Interoperability Continuum***, plus a **security element** that accounted for cybersecurity



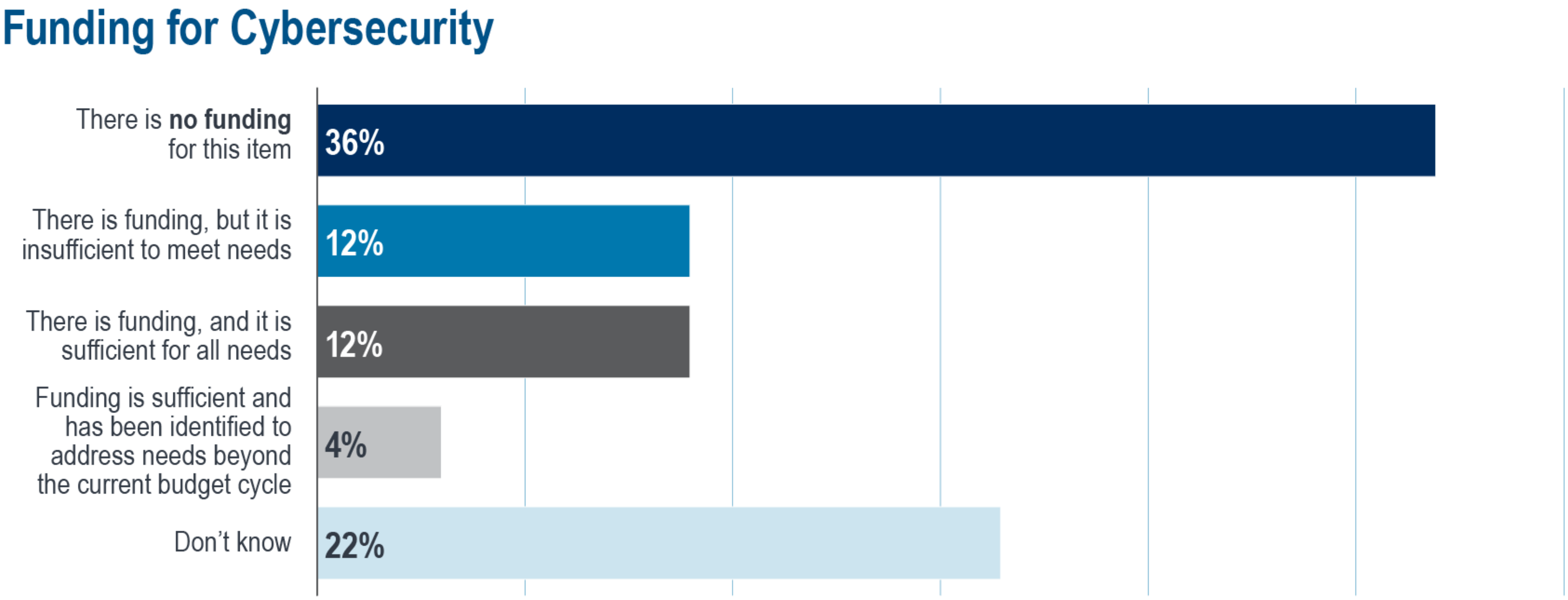
Cybersecurity Overview

Almost half of SNS respondents reported that a cybersecurity disruption or breach had an effect on their ability to communicate

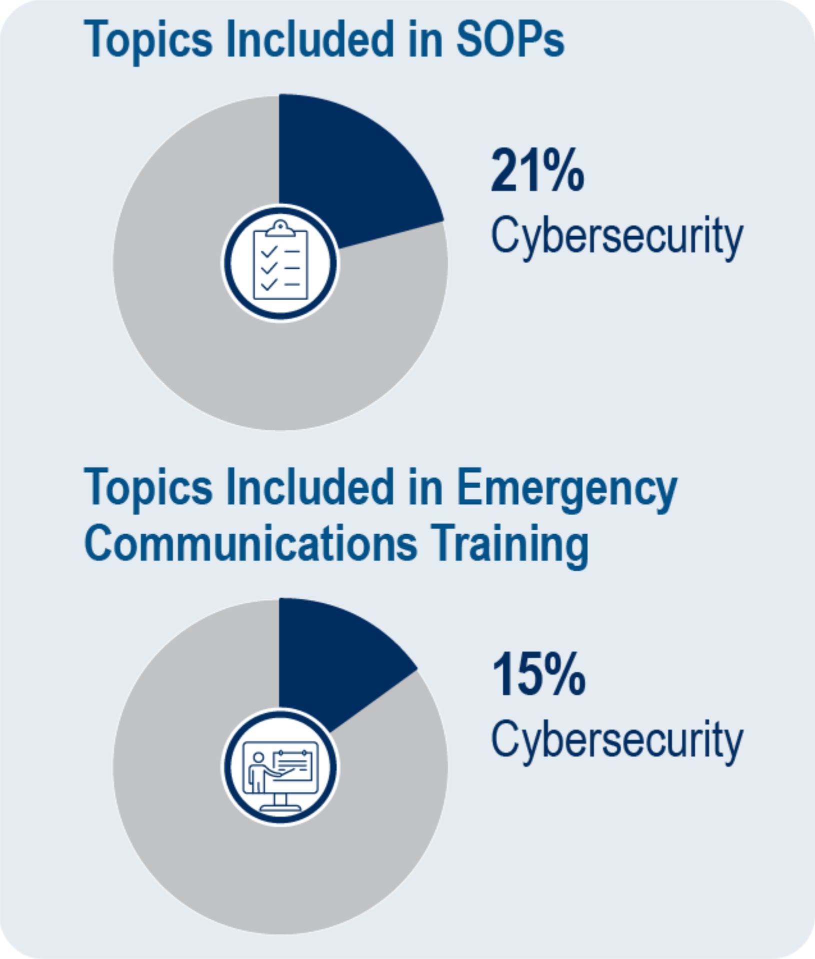
Factors that Affect Ability to Communicate: Cybersecurity Disruption or Breach



SNS: Cybersecurity Funding



SNS: Cybersecurity Additional Insights

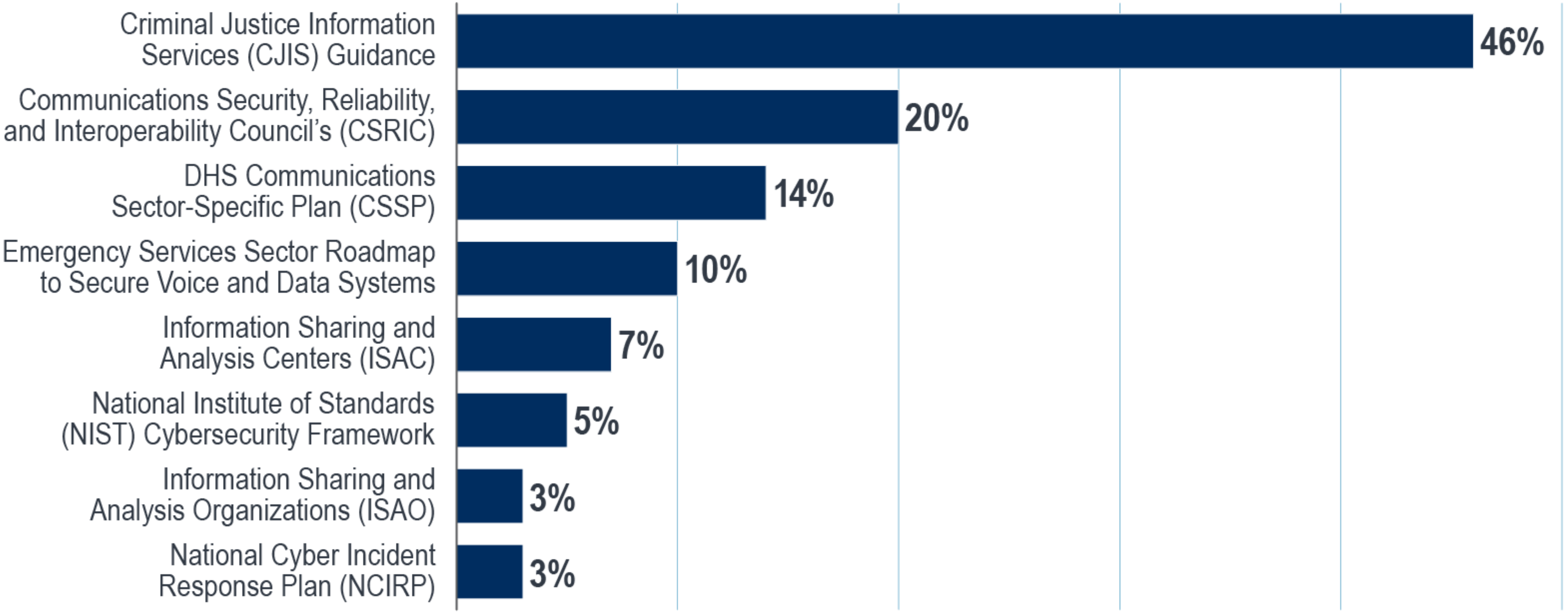

Topics Included in SOPs

Topics Included in Emergency Communications Training

Organizations reported that cybersecurity is not prioritized as a topic for Standard Operating Procedures (SOPs) and is often not included in Training and Exercise topics

SNS: Cybersecurity Additional Insights

Cybersecurity Guidelines and Standards Influencing SOPs



NECP Goal 6: Cybersecurity

Strengthen the cybersecurity posture of the Emergency Communications Ecosystem

- Objective 6.1: Develop and maintain cybersecurity risk management
- Objective 6.2: Mitigate cybersecurity vulnerabilities
- Objective 6.3: Determine public safety-specific, standards-based cyber hygiene minimums and fund ongoing risk mitigation

Additional Cybersecurity Success Indicators

Goal 1

Governance & Leadership

- Include cybersecurity representatives in governance bodies

Goal 2

Planning & Procedures

- Educate public safety agencies on cybersecurity risk mitigation
- Develop and maintain a cyber incident response plan

Goal 3

Training, Exercises, & Evaluation

- Update training and exercise programs to address cybersecurity

Panel Discussion

Charlie Guddemi
District of Columbia Homeland Security and Emergency Management Agency

Teddy Kavaleri
District of Columbia Office of Unified Communications

Karla Jurrens
Texas Department of Public Safety

Joseph Oregón
Cybersecurity and Infrastructure Security Agency, Region 9

Resources

- National Emergency Communications Plan
- SAFECOM Nationwide Survey
- CISA Public Safety Communications and Cyber Resiliency Toolkit
- CISA Cyber Incident Response
    - Cybersecurity Incident & Vulnerability Playbooks
    - CISA Incident Response Training
    - National Cyber Incident Response Plan
    - National Cybersecurity Protection System

Additional Resources

- CISA Cyber Essentials Toolkits
- Cybersecurity Evaluation Tool (CSET) Demonstration for Public Safety
- CISA Regional Offices
- Department of Homeland Security (DHS) Cybersecurity Services Catalog for State, Local, Tribal, and Territorial Governments
- U.S. Computer Emergency Readiness Team (US-CERT)
- National Institute of Standards & Technology (NIST) Cybersecurity Framework
- National 911 Program
- Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy Resource Center

Additional Resources

- CISA specific technology or attack vector guidance:
  - Transition to Next Generation 911
    - Two Things Every 911 Center Should Do To Improve Cybersecurity
    - Malware Attacks: Lessons Learned from an Emergency Communications Center
    - Cyber Incident Response to Public Safety Answering Points: A State's Perspective
    - Telephony Denial of Service Attacks: Lessons Learned from a Public Safety Answering Point
  - Cyber Risk to Public Safety: Ransomware
  - Cyber Risks to Land Mobile Radio - First Edition
  - Radio Frequency Interference Best Practices Guidebook

Additional Resources

- CISA Public Safety Communications Dependencies on Non-Agency Infrastructure and Services
  - Communications Dependencies Case Study: 2020 Midwest Derecho
  - Communications Dependencies Case Study: Nashville Christmas Day Bombing

How You Can Take Action

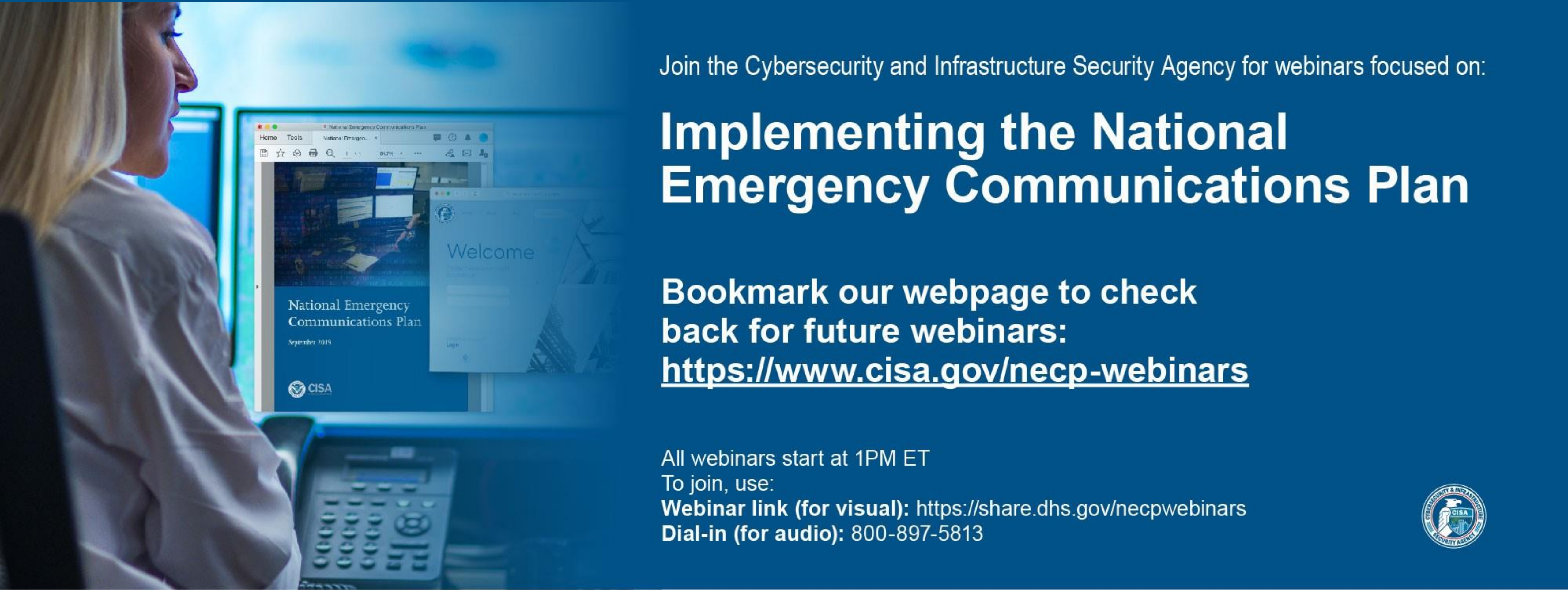
- **Take steps** for your organization or jurisdiction to implement the NECP and achieve its success indicators
- **Prioritize emergency communications needs** and coordinate with the SWIC to develop and maintain cyber incident response plans
- **Coordinate** with stakeholders and service providers to develop joint mutual agreements on continuity of operations during a cyber incident
- **Leverage** existing resources to support and maintain cyber incident response plans

SAFECOM® NATIONWIDE SURVEY

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

Questions?

Upcoming Webinars


Home
Tools
Welcome
National Emergency Communications Plan
September 2019
CISA

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

All webinars start at 1PM ET
To join, use:
Webinar link (for visual): https://share.dhs.gov/necpwebinars
Dial-in (for audio): 800-897-5813

For more information on the NECP:
www.cisa.gov/necp
NECP@cisa.dhs.gov

CYBERSECURITY & INFRASTRUCTURE

CISA

SECURITY AGENCY