THE NATIONAL EMERGENCY COMMUNICATIONS PLAN

THE IMPORTANCE OF PUBLIC SAFETY COMMUNICATIONS

Eric Runnels
Acting Associate Director, National Planning and Policy Sub-Division
Emergency Communications Division

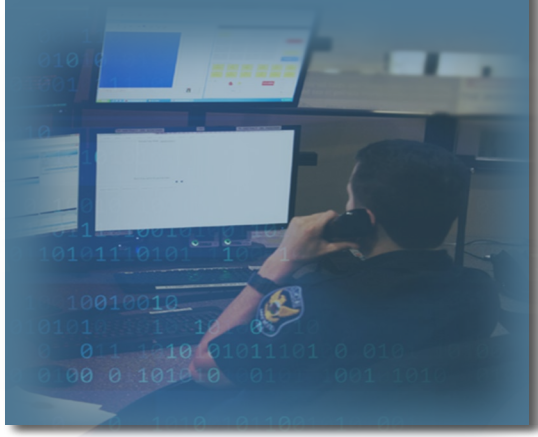
We Are CISA

VISION:
Secure and resilient critical infrastructure for the American people.

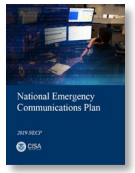
MISSION:
Lead the national effort to understand and manage cyber and physical risk to our critical infrastructure.

"Defend Today, Secure Tomorrow"
Emergency Communications

VISION	MISSION
Interoperable, secure, and resilient emergency communications enable daily operations and incident response throughout the Nation	Advance emergency communications in partnership with Public Safety and National Security/Emergency Preparedness communities



Statutory Authorities



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

Nationwide 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

Who CISA Supports

900K
Police Officers

825K
EMS Professionals

1.9M
Fire Personnel

1,200
Certified Emergency Managers

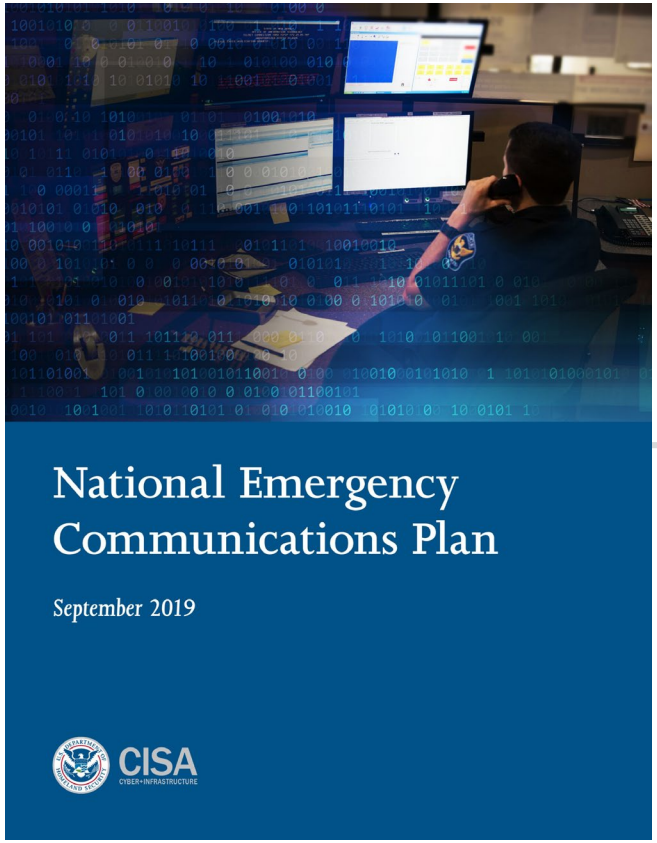
566
Federally Recognized Tribal Nations

19,400
Municipalities, Governors, Mayors, Public Works, Council Members

5,700 Hospitals
6,800 Banks
7,000 Power Plants
1,000 Wireline Carriers

Critical Infrastructure

National Emergency Communications Plan



- Mandated by Title XVIII of the Homeland Security Act of 2002, the NECP was first published in 2008, and its latest update was published in 2019
- The NECP is the Nation's strategic plan to strengthen and enhance emergency communications capabilities
- The Plan is designed to provide guidance to those that plan for, coordinate, maintain, invest in, and use communications to support public safety operations
- It helps stakeholders enhance and update the policies, governance structures, planning, and protocols that enable responders to communicate and share information under all circumstances
- The NECP navigates the complex mission of maintaining and improving emergency communications while also integrating new technologies and capabilities for emergency responders

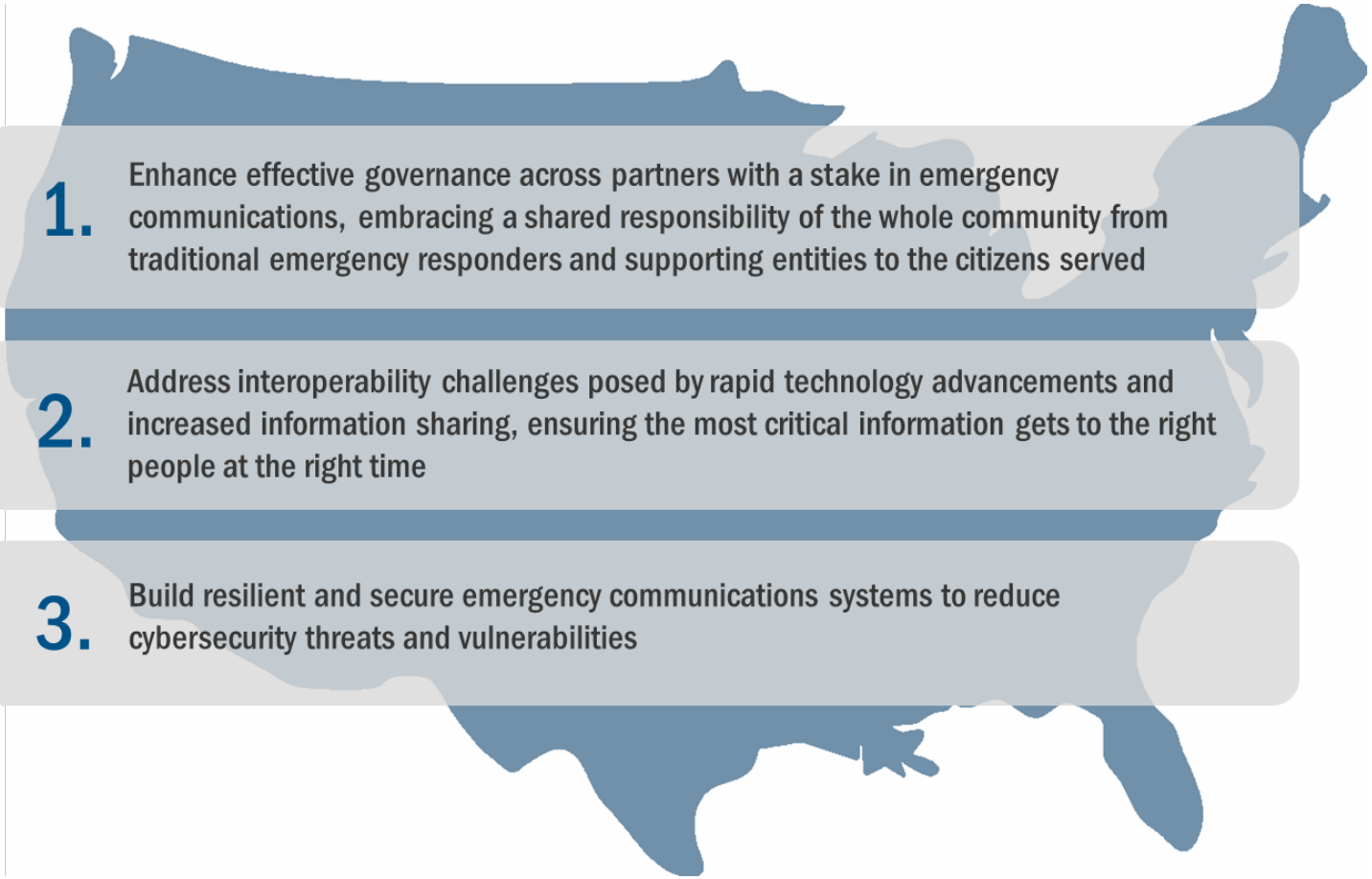
Updating the NECP

- The process for updating the NECP was stakeholder-driven and the updates are based on their input and feedback.
- Participation through:
  - SAFECOM Nationwide Survey
  - National Feedback Period
  - SAFECOM
  - Emergency Communications Preparedness Council (ECPC)
  - National Council of Statewide Interoperability Coordinators (NCSWIC)
  - Working Groups
  - Association Engagements
  - Webinars

The updated NECP addresses emergency communications gaps, reflects new and emerging technological advancements, and provides guidance to drive the Nation towards a common end-state for communications

NECP Vision and National Priorities

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

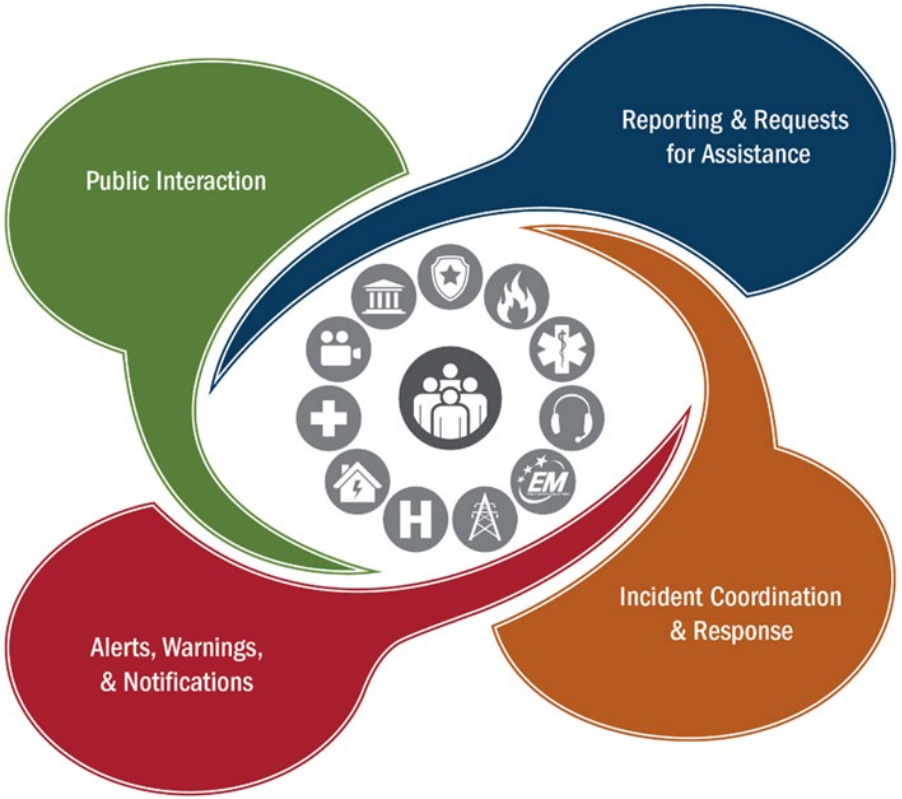


1. Enhance effective governance across partners with a stake in emergency communications, embracing a shared responsibility of the whole community from traditional emergency responders and supporting entities to the citizens served

2. Address interoperability challenges posed by rapid technology advancements and increased information sharing, ensuring the most critical information gets to the right people at the right time

3. Build resilient and secure emergency communications systems to reduce cybersecurity threats and vulnerabilities

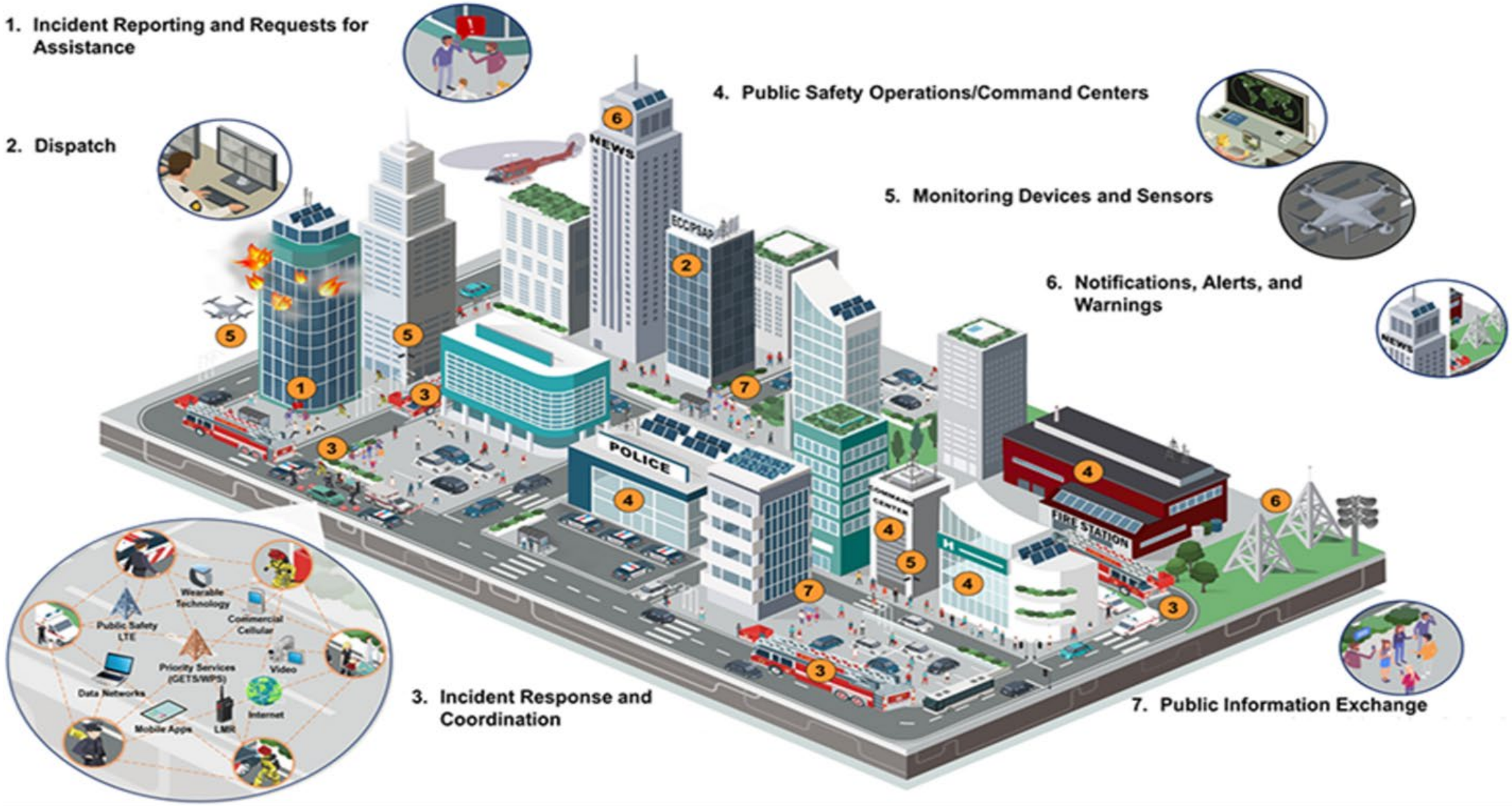
Emergency Communications Ecosystem



Communications Functions	Purpose	Examples
Reporting & Requesting Assistance	Urgent and non-urgent requests or information sharing made to public safety resources using defined emergency and non-emergency paths	911, 311, dedicated numbers, tip lines, alarm activated, face-to-face, triggered telematics system, social media, web applications, detection of service outages or disruptions
Incident Coordination & Response	Direct voice and data communications among public safety responders, emergency communication centers/public safety answering points, and emergency support systems to establish command and control, situational awareness, and shared common operating picture	Information sharing, joint planning, radio communications, in-field operations, data exchange
Alerts,Warnings, & Notifications	Instructional messages directing protective actions to save lives and property, and convey time-sensitive information for preparation, response, and recovery-related services	Active threats or civil dangers, hazmat, AMBER alerts, weather watches, fire warnings, evacuation orders, area accessibility updates, all-clear notices, Emergency Alert System, Wireless Emergency Alerts
Public Interaction	Public's sharing of information through various public or commercial networks supporting the Internet, social media, and telephony communications	Telephone calls, social media, such as Facebook, Twitter, web services and applications

- The Emergency Communications Ecosystem explains the various people and functions that exchange information prior to, during, and after incidents and planned events

Emergency Communications Ecosystem in Action



NECP Goals

Goal 1: Governance and Leadership

Develop and maintain effective emergency communications governance and leadership across the Emergency Communications Ecosystem

Goal 2: Planning and Procedures

Develop and update comprehensive emergency communications plans and procedures that address the evolution of risks, capabilities, and technologies across the Emergency Communications Ecosystem

Goal 3: Training, Exercises, and Evaluation

Develop and deliver training, exercise, and evaluation programs that enhance knowledge and target gaps in all available emergency communications technologies

Goal 4: Communications Coordination

Improve effective coordination of available operable and interoperable public safety communications capabilities for incidents and planned events

Goal 5: Technology and Infrastructure

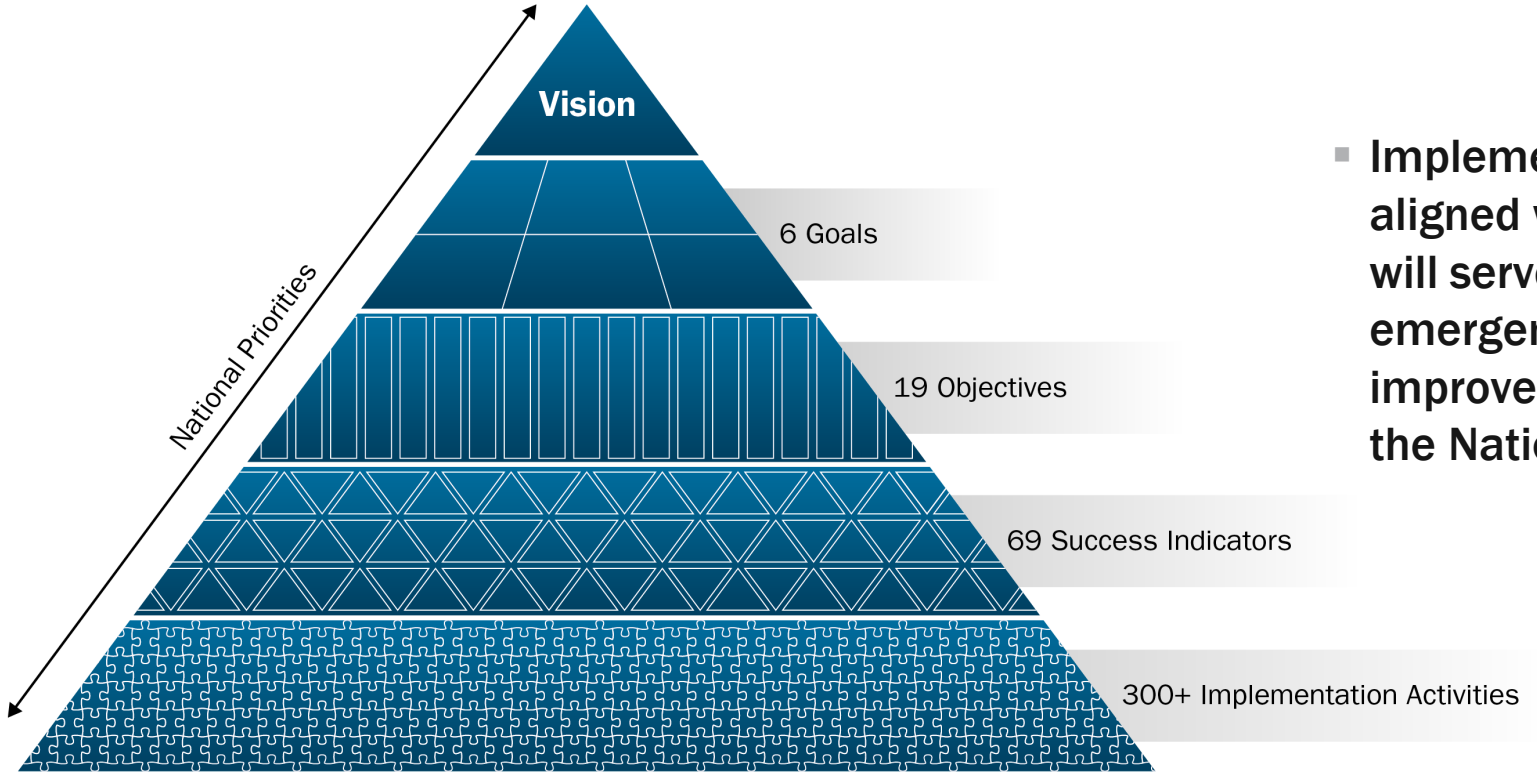
Improve lifecycle management of the systems and equipment that enable emergency responders and public safety officials to share information efficiently and securely

Goal 6: Cybersecurity

Strengthen the cybersecurity posture of the Emergency Communications Ecosystem

NECP Implementation Strategy

The NECP Implementation Plan is built upon a foundation of implementation activities and work plans that will help the Nation achieve the NECP's goals and objectives.



- **Implementation activities are aligned with success indicators and will serve as the catalysts for driving emergency communications improvements across the Nation.**

DoD and the NECP

DoD is supporting NECP implementation through the Emergency Communications Preparedness Center (ECPC). Implementation activities include:

- Establish a federal interoperability office or designating a Federal Interoperability Coordinator;
- Develop federal emergency communications strategic plans;
- Identify opportunities for federal interagency training and exercise programs;
- Coordinate federal research, development, testing, and evaluation priorities and processes; and
- Partner with the private sector to foster an open, innovative, and standards-based commercial marketplace for solutions development and ensures that public safety requirements are addressed in current and emerging standards

Ongoing NECP Implementation Support

DoD can continue to support NECP implementation by:

- Active engagement through the ECPC on the NECP implementation activities;
- Drawing connections between NECP planning and procedures objectives and related DoD emergency communications initiatives;
- Helping CISA understand how planned DoD initiatives support NECP training and exercise objectives so CISA can advocate the benefits and value of DoD; and
- Encouraging DoD to implement and actively use National Incident Management System doctrine and the National Institute of Standards and Technology Cybersecurity Framework

Implementing the NECP Webinars

PURPOSE: Provide practical solutions and resources to help organizations implement the NECP

Objectives:

Close Critical Emergency Communications Gaps

- Provide actionable steps and resources to address capability gaps identified in the NECP
- Review key findings from the SAFECOM Nationwide Survey to show stakeholders how they were addressed in the NECP

Target the Whole Community

- Invite the entire Emergency Communications Ecosystem to participate
- Employ an expansive outreach campaign (Web, email, social media) to reach the greatest audience
- 113,000+ public safety organizations targeted through email distribution lists

Foster Collaborative Partnerships

- Leverage the expertise of public safety organizations
- Demonstrate that emergency communications is a shared responsibility

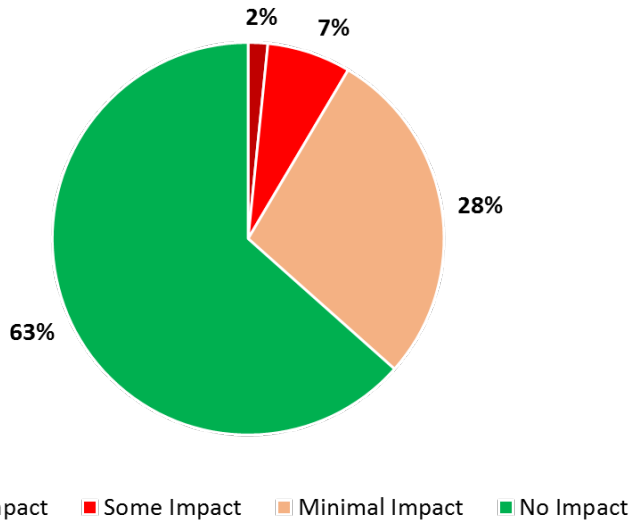
Upcoming Webinar

NECP Team
CISA Emergency Communications Division
Email: NECP@cisa.dhs.gov

Backup Slides

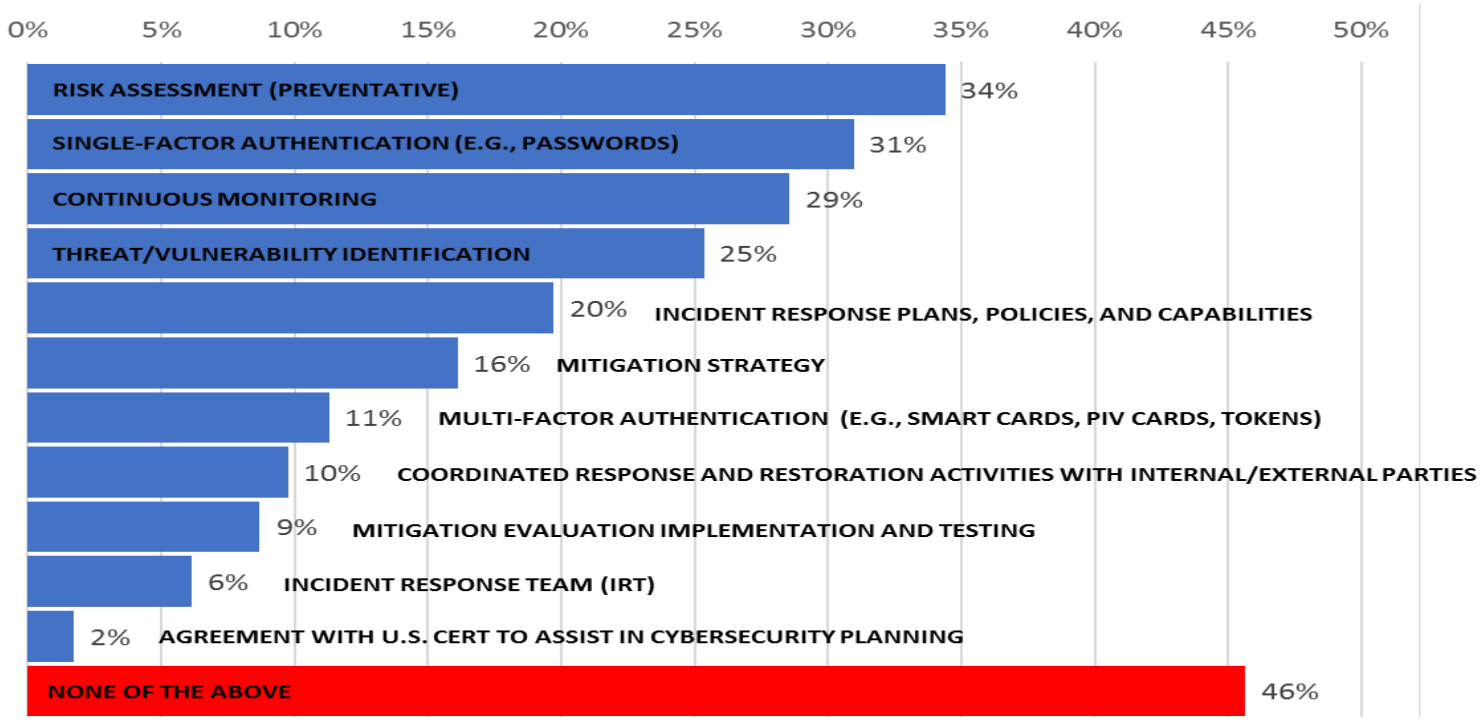
SNS: Cybersecurity Impact and Planning

Cybersecurity Impact



- Over a third of respondents indicated that cybersecurity incidents have had an impact on the ability of their emergency response providers and government officials' ability to communicate over the past five years

Elements that Organizations Incorporate into Cybersecurity Planning

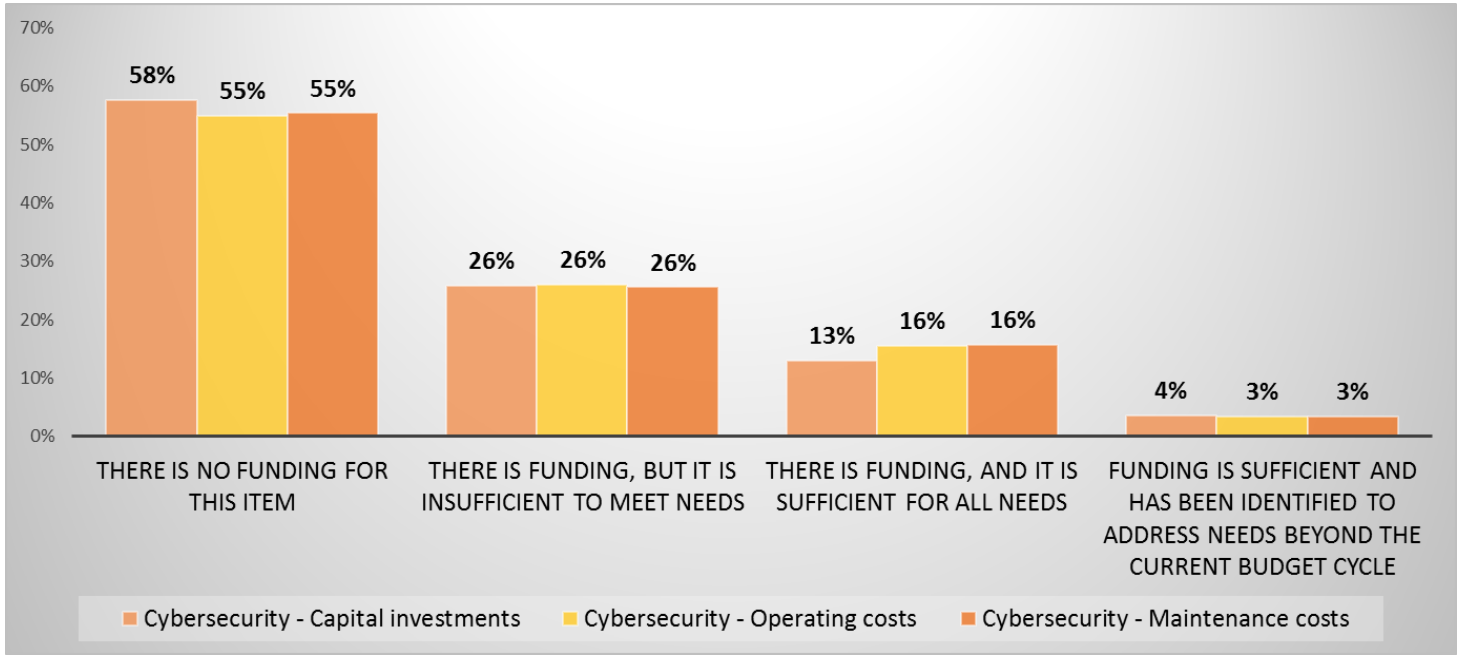


- 46% of organizations do not incorporate the listed cybersecurity measures into their cybersecurity planning
- Almost 60% of public safety disciplines located in rural areas do not participate in cybersecurity planning

SNS: Cybersecurity Funding and SOPs

- 16% of organizations reported that cybersecurity is not prioritized as a topic for Standard Operating Procedures (SOPs)
- 9% reported that it is not included in Training and Exercise topics
- Over 55% of organizations indicated that they don't have funding for cybersecurity capital investments or operating and maintenance costs
- Additionally, 26% of organizations indicated that their cybersecurity funding is insufficient to meet their needs

Funding for Cybersecurity



CYBERSECURITY & INFRASTRUCTURE
SECURITY AGENCY
CISA