



THE NATIONAL EMERGENCY COMMUNICATIONS PLAN (NECP) 2019 UPDATE



THE 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.

READ

To download the updated NECP, visit: www.cisa.gov/necp

SOCIAL MEDIA

- www.facebook.com/homelandsecurity/
- @CISAgov
- www.linkedin.com/company/cybersecurity-and-infrastructure-security-agency

Tag us on social media: #NECP2019



THE NECP 2019 UPDATE OVERVIEW

The National Emergency Communications Plan (NECP) is the Nation's strategic plan to strengthen and enhance emergency communications capabilities. The Cybersecurity and Infrastructure Security Agency (CISA) worked with over 3,500 Federal, state, local, tribal and territorial public safety agencies and organizations to develop the NECP. As a result, the updated NECP addresses the current gaps within emergency communications and promotes the innovation and integration of new technologies, while considering their associated risks. In addition, it provides guidance to drive the enhancements of the Nation's emergency communications capabilities. Some of the updates to the NECP, include:



A Cybersecurity Goal

As cyber threats and vulnerabilities grow in complexity and sophistication, it is critical that public safety organizations take proactive measures to manage their cybersecurity risks.



A Technology & Infrastructure Goal

This goal builds upon the previous Research and Development Goal and expands to cover key data interoperability, NG911, and FirstNet considerations.



A Focus on Adaptive Governance Strategies

Organizations can strengthen governance structures by embracing adaptive governance models that are flexible and support collaborative decision-making and by expanding membership composition (e.g. tribes, private sector, military).



Advocacy for Updated Training and Exercise Programs

To address new technologies, cyber threats, and organization-specific planning needs, it is recommended that organizations continue to expand training and exercise participation and content to improve operational policies and procedures.



Expanded Concept of Communications Resiliency

The concept has 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

It is recommended that organizations establish and maintain a repeatable process to periodically observe and record user proficiency for communications systems.

THE NECP PRIORITIES



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



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



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



WHOLE COMMUNITY PARTNERS

The NECP provides guidance to those that plan for, coordinate, invest in, and use communications to support response and recovery operations:

-  Law Enforcement
-  Fire
-  Emergency Medical Services
-  Emergency Comms Centers/PSAPs
-  Emergency Management
-  Public Works & Services
-  Public Health & Medical Facilities
-  Transportation Agencies, Utilities, Critical Infrastructure Operators, & Commercial Service Providers
-  Nongovernmental Organizations, Auxiliary Resources, & International Partners
-  Media
-  Private citizens
-  Elected and Appointed Officials; Federal, State, Local, Tribal, and Territorial Governments, and Regional Authorities

THE NECP GOALS

1 GOAL 1: Governance & Leadership

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

2 GOAL 2: Planning & Procedures

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

3 GOAL 3: Training, Exercises, & Evaluation

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

4 GOAL 4: Communications Coordination

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

5 GOAL 5: Technology & Infrastructure

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

6 GOAL 6: Cybersecurity

Strengthen the cybersecurity posture of the Emergency Communications Ecosystem

THE ECOSYSTEM

The Emergency Communications Ecosystem is comprised of the various functions and people that exchange information prior to, during, and after incidents. As emergency responders integrate new technologies with existing systems, response agencies become more connected through additional sources of information. As a result, the communications functions within the Ecosystem become increasingly interwoven and complex.

The key functions necessary to achieve reliable, secure, and interoperable emergency communications include: *Reporting and Requests for Assistance*, *Incident Coordination and Response*, *Alerts, Warnings, and Notifications*, and *Public Interaction*.

Information can flow multiple directions within the primary functions and may be initiated by any whole community partner, depending on the nature of the event or incident.

