



2019 Update

NATIONAL EMERGENCY COMMUNICATIONS PLAN

FREQUENTLY ASKED QUESTIONS

Background, Updates, and Changes

1. What is the National Emergency Communications Plan (NECP)?

The NECP is the Nation’s strategic plan to strengthen and enhance emergency communications capabilities. The NECP sets forth a vision for the current and future state of emergency communications nationwide, and aims to ensure resilient, secure, operable, and interoperable communications among organizations during emergencies. To achieve this vision, the NECP establishes goals and objectives and provides success indicators to improve communications between emergency response providers and relevant government officials in the event of disasters and acts of terrorism.

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. ”

2. Why was the NECP updated?

Title XVIII of the Homeland Security Act of 2002, as amended, requires the Cybersecurity and Infrastructure Security Agency (CISA) to periodically update the NECP. Additionally, the 2018 SAFECOM Nationwide Survey (SNS) reflected the need to address specific challenges around emerging technologies, new capabilities, and new partners. Some of the other drivers of change include land mobile radio (LMR) to long-term evolution (LTE) integration, the expanded use of broadband technologies, targeted alerts and warnings, the transition to Next-Generation 911 (NG911), the deployment of FirstNet, increasingly complex emergencies, and the need to strengthen cybersecurity to ensure the availability and integrity of communications and information during incident and hazards events.

3. What are the NECP’s Goals?

Updates to the goals in the NECP build upon the foundational concepts of the prior versions and address evolving challenges such as increasingly complex emergencies, rapid technological advancements, data interoperability, the integration and alignment of technologies, and cybersecurity.

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

DRIVERS OF CHANGE

Within the Emergency Communications Landscape



LMR-LTE Integration



Expanding Use of Broadband Technologies



Targeted Alerts and Warnings



Transition to NG911



Deployment of FirstNet



Increasingly Complex Emergencies



Strengthening Cybersecurity Posture



Increasing Public Engagement



Evolving Roles of Communications Personnel



Data Interoperability



Background, Updates, and Changes (Continued)

4. How was the updated NECP developed?

CISA engaged more than 3,500 public safety representatives from federal, state, local, tribal, and territorial public safety agencies; NGOs; the private sector; and other groups through interviews, public webinars, working groups, and a national feedback period. In addition, CISA leveraged lessons learned from 2008 and 2014 NECP implementation, real-world events, results from the 2018 SNS and the 2018 Nationwide Communications Baseline Assessment, and partnerships from the communications and information technology sectors to update the NECP’s goals, objectives, and success indicators.

5. How has the NECP changed?

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:



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, the NECP recommends that organizations continue to expand training and exercise participation and content to improve operational polices and procedures.



Cybersecurity Goal

The NECP advocates for increased cybersecurity and encourages public safety organizations to take proactive measures to manage cyber threats and vulnerabilities.



Technology and Infrastructure Goal

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



Increased Emphasis on Strengthening Communications Resiliency

The NECP encourages periodic testing and user-usage observations, active resource sharing, and regionalization of shared infrastructure, networks, and services to ensure continuity of communications throughout operations.



Recommendations for Enhanced Communication Coordination

The NECP recommends that organizations establish and maintain a repeatable process to periodically observe and record user proficiency for communications systems.

6. Who is the NECP’s intended audience?

The NECP is written for those personnel who plan for, coordinate, invest in, and use communications to support response and recovery operations. This includes traditional emergency responder disciplines (e.g., law enforcement, fire, emergency medical services, dispatch) and other entities that share information during emergencies, such as medical facilities, utilities, nongovernmental organizations, as well as the media and private citizens. The NECP is also designed to help decision-makers who are responsible for setting mission priorities, developing budgets, and planning for and acquiring communications technology assets. For more information, contact NECP@cisa.dhs.gov.

Whole Community Partners



Law Enforcement

- Fire
- Emergency Medical Services
- Emergency Communication Centers/Public Safety Answering Points
- Emergency Management
- Public Works and Services
- Public Health and Medical Services
- Transportation Agencies, Utilities, Critical

Infrastructure Operators, and Commercial Service Providers

- Nongovernmental Organizations, International Partners, and Auxiliary Resources
- Media
- Private Citizens
- Elected and Appointed Officials; Federal, State, Tribal, and Territorial Governments; and Regional Authorities

*Listed entities reflect a sample of potential partners and do not represent a comprehensive list.

Background, Updates, and Changes (Continued)

7. What are the updated NECP National Priorities?

- ✓ Enhance effective governance across partners with a stake in emergency communications by diversifying membership of governance bodies
- ✓ Address interoperability challenges posed by rapid technology advancements and increased data sharing
- ✓ Build resilient and secure emergency communications systems to reduce cyber threats and vulnerabilities

8. Who is responsible for implementing the NECP?

NECP implementation is a shared responsibility among the plan's stakeholders. This shared approach reflects the nature of the emergency response community, which spans disciplines, jurisdictions, levels of government, and involves the public and private sectors. Successful implementation relies on the support and dedication of the entire emergency response community.

Leveraging the NECP

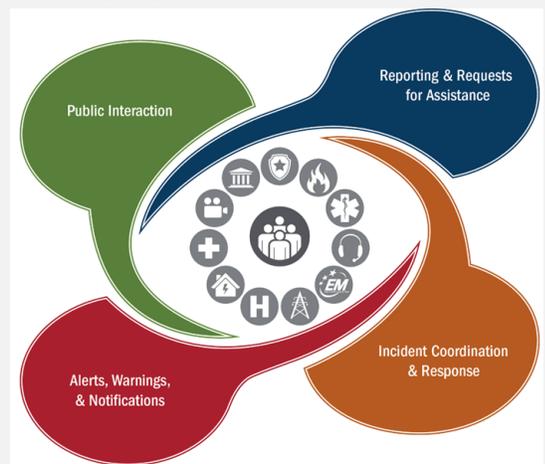
9. How does the NECP fit into the broader national preparedness strategy?

The NECP is a key component of the Nation's preparedness portfolio as it aligns, implements, and supports national strategies to enhance preparedness and resilience. This includes, but is not limited to, Presidential Policy Directive-8, the National Preparedness Goal, the National Preparedness System, the National Planning Frameworks, the National Incident Management System, and the National Infrastructure Protection Plan. These authorities and initiatives set national policy and provide executive direction in areas closely related to emergency communications, such as national preparedness, domestic incident management, critical infrastructure resilience, cybersecurity, and continuity of government operations. Implementation of the NECP in conjunction with other preparedness directives, statutes, policy, and doctrine can further ensure that the public safety community is collectively driving towards a common end-state for communications.

10. How does the NECP address new technologies?

New and emerging technologies provide the public safety community with advanced capabilities to enhance command, control, and situational awareness. However, they have the potential to disrupt mission-critical operations and introduce new risks, such as system failure, cyber-attacks, and data breaches. As a result, the updated NECP places an increased emphasis on accelerating research, development, testing, evaluation, and standards implementation for emerging technologies to meet public safety's critical needs. The updated NECP also continues to prioritize maintenance of land mobile radio and data exchange systems, while embracing new capabilities. The NECP's Goal 5 was also renamed from *Research and Development* to address the broadened scope of technology and infrastructure to account for the full technology lifecycle, from identification of research and development opportunities to the graceful disposition of systems.

Emergency Communications Ecosystem



Reporting & Requesting Assistance

Urgent and non-urgent requests or information sharing made to public safety resources using defined emergency and non-emergency paths

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

Alerts, Warnings, & Notifications

Instructional messages directing protective actions to save lives and property, and convey time-sensitive information for preparation, response, and recover-related services

Public Interaction

Public's sharing of information through various public or commercial networks supporting the Internet, social media, and telephony communications



Leveraging the NECP (continued)

11. How should stakeholders use the NECP?

Based on a stakeholder’s capabilities, needs, and strategic direction, they can incorporate the NECP’s vision, priorities, and goals within their own strategic planning efforts, such as the Statewide Communication Interoperability Plans (SCIPs) or agency-specific strategic plans. Additionally, the NECP defines Success Indicators for each objective, which describe the desired future state of communications. Stakeholders can leverage the success indicators to identify appropriate actions to meet their unique needs and missions and measure progress until success indicators are a reality. Additional NECP resources can be found at www.cisa.gov/necp.

NECP Resources

12. What federal resources are available to implement the NECP?

To assist stakeholders with NECP implementation, technical assistance and stakeholder workshops are available for NECP partners to support their emergency response resource allocations and decision-making. Although there is no large-scale grant program dedicated to NECP implementation, there are various federal grants and resources available to fund emergency communications activities, which include planning, personnel, training, exercises, and equipment. Such funding opportunities are made available by federal agencies, including the Department of Justice Community Oriented Policing Services, the Department of Health and Human Services Assistant Secretary for Preparedness and Response, and the Federal Emergency Management Agency, among others. To view additional funding resources to help maintain interoperable networks, and to learn how to apply for emergency communications funding, please visit www.dhs.gov/safecom/funding.

13. What services will CISA and its partners provide to stakeholders to support NECP implementation?

- Emergency Communications Coordination
- Interoperable Communications and Technical Assistance Program
- Priority Telecommunications Services
- Statewide Communication Interoperability Plan (SCIP) Workshops
- Stakeholder Collaboration

CISA and its stakeholder partners are developing additional emergency communications guidance documents and publications. To view the latest resources, visit <https://www.cisa.gov/emergency-communications-guidance-documents-and-publications>.

14. How is the FY 2020 SAFECOM Guidance on Emergency Communications Grants aligned to the NECP?

CISA developed the *SAFECOM Guidance on Emergency Communications Grants* in partnership with SAFECOM and NCSWIC to address the evolving Emergency Communications Ecosystem and encourage grant recipients to support the concepts and recommendations outlined in the NECP. The *SAFECOM Guidance on Emergency Communications Grants* serves as a reference guide for those applying for federal financial assistance and provides stakeholders with the latest information on eligible activities, technical standards, and other terms and conditions that are common to most federal emergency communications grants.

The *SAFECOM Guidance on Emergency Communications Grants* aims to help state, local, tribal and territorial stakeholders develop projects that adequately address the NECP’s three national priorities and help ensure federally-funded investments support the enhancement of secure, interoperable emergency communications.

To download the *SAFECOM Guidance on Emergency Communications Grants*, visit www.dhs.gov/safecom/funding.

THE NECP Online Resources

A copy of the NECP is available for download at <https://www.cisa.gov/necp>.
For more information on the NECP, email us at necp@cisa.dhs.gov.