THE NATIONAL EMERGENCY COMMUNICATIONS PLAN: FREQUENTLY ASKED QUESTIONS

BACKGROUND, UPDATES, AND CHANGES

1. What is the NECP?

The National Emergency Communications Plan (NECP) is the nation's strategic plan to strengthen and enhance emergency communications capabilities. It establishes 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 identifies 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.

2. What are the goals of the NECP?

There are six goals of the NECP including Goal 1: Governance and Leadership, Goal 2: Planning and Procedures, Goal 3: Training, Exercises and Evaluation, Goal 4: Communications Coordination, Goal 5: Technology and Infrastructure, and Goal 6: Cybersecurity. Each goal is aligned with three to four objectives that include specific deliverables in support of the corresponding goal.

NECP Goals

Goal 1: Governance and Leadership

Goal 2: Planning and Procedures

Goal 3: Training, Exercises, and Evaluation

Goal 4: Communications Coordination

Goal 5: Technology and Infrastructure

Goal 6: Cybersecurity

3. How has the NECP changed over time?

First published in 2008, and updated in 2014 and 2019, the NECP continually evolves to meet the needs of the emergency communications community. The NECP prepares stakeholders for rapid technological change and its associated risks by addressing current challenges and identifying opportunities for improving emergency communications capabilities in technology, infrastructure, and cybersecurity. The NECP also seeks to enhance governance structures, adopt common policies and procedures, expand training and exercise programs, migrate legacy systems, integrate new technologies, and mitigate growing cyber threats.

4. Who is the NECP's intended audience?

The NECP is written for those 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.

5. Who is responsible for implementing the NECP?

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

Whole Community Partners

- Law Enforcement
- Fire
- Emergency Medical Services
- Emergency Communication Centers
- Emergency Management
- Public Works and Services
- Public Health and Medical Services
- Private Citizens

- Media
- Nongovernmental Organizations, International Partners, and Auxiliary Resources
- Transportation Agencies, Utilities, Critical Infrastructure Operators, and Commercial Service Providers
- Elected and Appointed Officials; Federal, State, Tribal, and Territorial Governments; and Regional

LEVERAGING THE NECP

6. 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 the preparedness and resilience of the nation. This includes, but is not limited to, Presidential Policy Directive (PPD)-8, the National Preparedness Goal, the National Preparedness System, the National Planning Frameworks, the National Incident Management System (NIMS), and the National Infrastructure Protection Plan (NIPP). 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.

7. How should stakeholders use the NECP?

Based on stakeholders' capabilities, needs, and strategic direction, they can leverage 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.

8. 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 NECP emphasizes accelerating research, development, testing, evaluation, and standards implementation for emerging technologies to meet public safety's critical needs. It also prioritizes maintenance of land mobile radio and data exchange systems, while embracing new capabilities. The NECP's Goal 5 (Technology and Infrastructure) accounts for the full technology lifecycle, from identification of research and development opportunities to the graceful disposition of systems.

NECP RESOURCES

9. What federal funding is 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 departments and agencies, including the Department of Justice Community Oriented Policing Services, the Department of Health and Human Services Assistant Secretary for Preparedness and Response, the Department of Agriculture Rural Utilities Services, the Federal Emergency Management Agency. To view a complete list of federal department and agency grant programs, and to learn how to apply for emergency communications funding, please visit: www.cisa.gov/safecom/funding.

10. How is SAFECOM Guidance on Grants aligned to the NECP?

The Cybersecurity and Infrastructure Security Agency (CISA), in partnership with SAFECOM and the National Council of Statewide Interoperability Coordinators, publishes the SAFECOM Guidance on Emergency Communications Grants yearly which assists state, local, tribal, and territorial governments planning or applying for federal financial assistance funding to invest in emergency communications projects.

This guidance pertains to emergency communications activities eligible for federal grants, best practices for improved interoperability, recommendations for coordinating and implementing projects, and resources to help recipients comply with grant requirements. The SAFECOM Guidance additionally encourages grant recipients to follow recommendations outlined by the NECP and take on projects that execute NECP priorities and promote NECP national goals. For more information on SAFECOM Guidance on Grants, visit SAFECOM Guidance on Grants.

11. What technical assistance is available to help implement the NECP?

CISA's Emergency Communications Division directly supports emergency responders and government officials in implementing NECP directives by developing and delivering training tools and providing onsite assistance to advance public safety interoperable communications capabilities. Service is provided at no cost and is available to state, local, and tribal governments in all 56 states and territories. CISA provides a portfolio of no-cost technical assistance services. To learn more about this technical assistance, you can visit the CISA Interoperable Communications Technical Assistance Program (ICTAP) page or email necp@cisa.dhs.gov.

NECP ONLINE RESOURCES

A copy of the NECP is available for download at www.cisa.gov/necp.
For more information on the NECP contact: necp@cisa.dhs.gov