THE NECP

National Emergency Communications Plan

NECP Spotlight:

Ensuring Interoperable Encrypted Communications

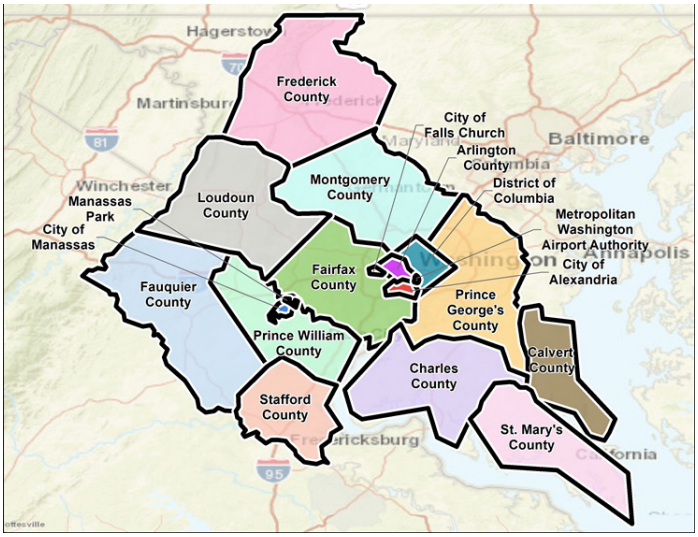
INTRODUCTION

Emergency responders rely on their radios every day to maintain communications with other agencies and jurisdictions. In life or death situations, it is critical that their communications are both reliable and secure. Encryption is one way public safety agencies are ensuring secure and effective radio communications in an increasingly digital environment. Encryption enables secure communication between parties by standardizing an encryption key across all radios assigned to a group. This key acts as a password that must be known to decrypt the call at the receiving end. While this protects critical information for tactical and operational security reasons, using encryption requires enhanced interoperability during joint emergency response efforts. First responders using encryption can achieve and maintain interoperability by having an encryption key management plan and ensuring coordination amongst surrounding jurisdictions.

The National Emergency Communications Plan (NECP) is the Nation's strategic plan to strengthen emergency communications and advocates for the incorporation of risk management strategies to protect against and mitigate disruptions to mission-critical communications. This spotlight will examine how emergency response agencies in the National Capital Region (NCR)—including multiple jurisdictions and agencies in Northern Virginia, Maryland, and Washington, D.C.—balance the need to protect critical information through encryption while also maintaining communications interoperability across jurisdictions. The region's efforts to develop the Public Safety Land Mobile Radio (LMR) Strategic Interoperable Encryption Plan (Encryption Plan) ensures radio interoperability locally, serving as an example of successfully implementing recommendations set forth in the NECP.

AN IN-DEPTH LOOK

The Encryption Plan was developed in response to Washington, D.C.'s decision to encrypt law enforcement radio communications. Without regional coordination, D.C.'s encrypted channels would prevent responding agencies outside the city from communicating with units inside the city. To retain communications interoperability, all NCR jurisdictions came together to develop a plan to ensure that emergency responders could transmit and receive voice, data, and video communications in both clear and encrypted modes.



Map of the National Capital Region[1]

The Encryption Plan was created through the Metropolitan Washington Council of Governments (MWCOG), specifically the Public Safety Communications Subcommittee which is governed by both the Police Chief's and Fire Chief's Emergency Support Function Committees. These committees enable police and fire chiefs to influence the region's approach to interoperability and policy.

The process used to develop the Encryption Plan helped all the jurisdictions within the NCR to jointly establish guidelines for migration to compatible 700/800 Megahertz (MHz) trunked public safety radio systems. These updated systems provide interoperability for public safety agencies during daily operations as well as disaster response though achieving interoperable encrypted communications continues to be a work in progress.

> "Goal One: Ensure emergency response providers of the Greater Metropolitan Washington Area have the ability to transmit and receive voice, data, and video communications in both clear and encrypted modes."
>
> — Public Safety LMR Strategic Interoperable Encryption Plan[2]

AN IN-DEPTH LOOK CONTINUED

Across the NCR, the Encryption Plan has been implemented alongside a regional Interoperable Communications Memorandum of Understanding (MOU) to enhance joint communications further. Federal Communications Commission requirements state that each jurisdiction must have a MOU with every regional partner with whom it shares communications information. To consolidate efforts and maintain interoperability, the region drafted one regional MOU with signatories from cities, counties, private sector agencies, and federal partners surrounding Washington D.C., including the Washington Metropolitan Area Transit Authority, Metropolitan Washington Airports Authority, and Amtrak.

NECP ALIGNMENT

Secure and resilient interoperable communications require the coordination and cooperation of all agencies and stakeholders who frequently work together during emergencies. By leveraging the NECP's recommendations, public safety agencies can ensure that emergency responders can communicate securely while still preserving communications interoperability. The following chart aligns specific NECP recommendations to real world examples highlighted in the NCR's implementation of the Encryption Plan.

NECP Goal	Objective	Objective Description	Real World Example
Goal 1: Governance and Leadership	1.3	Adopt adaptive governance strategies to address the rapid evolution of technologies, capabilities, and risks	The MWCOG Public Safety Communications Subcommittee coordinates regionally to address the evolution of radio encryption technologies and the Project 25 (P25) recommended NIST Compliant Advanced Encryption Standards.
Goal 2: Planning and Procedures	2.1	Develop and regularly update strategic plans to align with the NECP and address the integration of new emergency communications capabilities (e.g., voice, video, and data)	The MWCOG Public Safety Communications Subcommittees review and recommend changes to interoperable radio talk groups on a regular basis. Regional coordination and collaboration between public safety leaders and governance committees helps ensure the Encryption Plan addresses and resolves long-standing operability and interoperability issues.
Goal 4: Communications Coordination	4.2	Enhance coordination and effective usage of public safety communications resources at all levels of government	All local jurisdictions within the MWCOG have acquired compatible 700/800 MHz trunked public safety radio systems. Regional, state, and federal agencies can be interconnected to these agencies using multiple technologies.
Goal 6: Cybersecurity	6.2	Mitigate cybersecurity vulnerabilities	As jurisdictions within the NCR move from hardwire to Internet Protocol-based technologies, encryption becomes an essential part of their cybersecurity posture. The Encryption Plan provides emergency responders with the protocols and procedures to operate on encrypted radio channels or talk groups, prohibiting bad actors from hacking in and disrupting emergency communications.

RESOURCES

Encrypted radio channels allow emergency responders to protect mission-critical and sensitive information during emergency response. To learn more about how you can implement the recommendations in the NECP within your agency, visit: cisa.gov/necp.

Want to share your organization's successes and alignment to the NECP? Email us at: necp@cisa.dhs.gov.

Encrypted information is still available to the public through the Freedom of Information Act, but only after an incident has been resolved. To learn more about encryption and how to improve interoperability of emergency communications, visit: cisa.gov/publication/encryption.

[1] National Capital Planning Commission (2021). "National Capital Region Map."
[2] National Capital Region Joint Public Safety Communications Committee (2018). "National Capital Region (NCR) Public Safety - Land Mobile Radio Strategic Interoperable Encryption Plan."