
2025
Law Enforcement Report

Research and report provided as a law enforcement service from the office of the "National Law Enforcement and Community Policing Integrated Network" (NLECPIN)

# Breaking the Chain of Risk

## The Importance of Securing Law Enforcement Communication & Collaboration in the 21st Century

**I**n an era defined by complex threats and constant scrutiny, the integrity of law enforcement work increasingly hinges not just on how well officers do their jobs, **but how well they communicate and collaborate**. Yet across the country, many agencies and law enforcement officers are still relying on texts, emails, and open-source messaging apps to communicate and coordinate high-stakes investigations and operations.

These outdated practices jeopardize agencies and can harm officers' careers, negatively impact investigations, endanger public safety, undermine public confidence, and compromise prosecutions.

While many traditions and practices remain the bedrock of a proud law enforcement heritage, others must evolve; not to erase that legacy, but to safeguard and defend it. In today's environment, the modernization of collaborative policing is no longer a matter of convenience; it is a matter of survival. Our ability to protect the institutions we serve and the communities we have sworn to defend are at a critical crossroads. The moment for this change is not "sometime in the future" - it is now.

## When Convenience Becomes Liability

Despite explicit guidance from the FBI and the Department of Justice discouraging their use for official law enforcement work, personal cell phones, emails and consumer apps are still the go-to tools for law enforcement communication.

The consequences of continuing to use these outdated tools are real. Here are just a few examples of **many**:

- In late 2024, Las Vegas Metro officers were investigated for using the Signal app—an encrypted messaging platform with disappearing messages—for work-related communications, which violated department policy on record-keeping and transparency - emphasizing risks to accountability and potential evasion of public records laws like FOIA. (KNTV.com, 2024)
- In 2025, several Illinois officers were disciplined for using WhatsApp on personal phones to coordinate responses during a high-profile protest. This violated departmental and legal protocols requiring all work-related communications to be logged for transparency and accountability. (Chicago Tribune, 2025)
- The Camden County Police Department in New Jersey experienced a ransomware attack in 2023 that locked critical criminal investigative files and disrupted day-to-day administrative functions - highlighting email-related vulnerabilities. (GovTech.com, 2025)
- A recent 2019 Inspector General investigation into a failed federal-state operation in Texas found that "critical decisions were made via undocumented text messages between agencies," contributing to a compromised informant and the subsequent collapse of the investigation. (DOJ OIG Report, 2019)

An audit by the Police Executive Research Forum found that the majority of multi-agency law enforcement teams used personal messaging apps for operational communication, with little oversight, recordkeeping, or data security protocols in place.

> *That's not just a policy problem — it's a **legal** and **constitutional** risk."*

## When Communication Breaks Down, So Does Justice

The use of non-sanctioned, untraceable, unsecure, open-sourced or mixed communication has negatively impacted many aspects of policing:

- **Criminal Prosecutions:** The lack of documented communication or mixed personal and professional messaging has led to suppressed evidence or dismissed charges.
- **Officer Safety:** Unclear or delayed messages in operations put personnel in harm's way.
- **Public Accountability:** FOIA and State records requests and civil suits have uncovered that decisions are often made in ways the departments cannot explain or verify.

In high-profile court cases, defense attorneys are increasingly challenging prosecutions based on chain-of-command lapses, personal communications of officers and unlogged decision-making. For example, a Massachusetts State Police Trooper was fired in 2025 after personal texts sent from his private phone (which he also used to communicate and share official law enforcement business) surfaced during a high-profile murder investigation. The messages contained derogatory commentary about the defendant, undermining public confidence and contributing to a mistrial. (WGBH NEWS, 2025).

## Interagency Collaboration Is Now the Rule — Not the Exception

Law enforcement agencies and law enforcement officers do not work in a vacuum. Whether it's narcotics, missing persons, organized crime, or large-scale public events, the reality is that municipal, county, state, and federal agencies must coordinate in real time.

But too many agencies continue to improvise by using unstructured tools, relying on someone knowing the "right person" to text, email, or call. That kind of informal structure might seem to work or be "good enough," until it is not - and when it fails, **it fails big**.

What is needed is a government approved, secure, court compliant, law-enforcement-controlled platform that provides encrypted, trackable, and integrated communication and collaboration — not just within departments, but across agencies.

Government approved systems like the "National Law Enforcement and Community Policing Integrated Network" (OPS Network™ / OPS CONNECT™), currently in use in more than 600 federal, state, county and local law enforcement agencies across the United States, provide real-time dashboards, assignment tools, officer logs, broadcast notifications, alert sharing, group coordination and encrypted messaging — all within a **law enforcement and legally compliant ecosystem**. With a system like the OPS Network™, and its secure, law enforcement managed assets now available nationwide, the principle is clear: law enforcement needs to operate on a secure tool built specifically for law enforcement — not patched together from the civilian tech stack.

> *".....too many departments are still **improvising with unstructured tools** — and when it fails, it **fails big**."*

## The Stakes? Careers, Cases, and Communities

This is not about convenience or technical savvy. This is about protecting careers, preserving public trust, and ensuring justice is delivered without compromise. Phrases like “Well, that’s how it’s always been” or “Nobody likes change” reflect outdated practices that fail to address modern challenges and prefer comfort over accountability. These are not valid reasons; they are often excuses made by those unable or unwilling to recognize the urgency of the moment, until the consequences of inaction land directly at their doorstep.

- **Careers:** Officers have been disciplined and terminated for violating communication policies, even when their intentions were good. Using personal devices for official business exposes officers to public records requests, subpoena risk, personal liability and internal affairs investigations.
- **Community Safety:** Delayed or unclear communication via email or text during critical incidents can result in tactical failures, misallocated resources, or worst case, injuries and loss of life.
- **Investigations and Court Outcomes:** When decisions and communications are not documented in an approved system, prosecutors lose leverage, defense attorneys gain ground, and cases can fall apart.
- **Police Licensing:** As more and more states implement police licensing, these outdated modes of communications may fall short of the licensing standards and lead to licensing actions being brought against law enforcement officers. An adverse decision on a law enforcement officer’s license can lead to loss of employment and result in pension related sanctions.

## A Culture Shift Is Urgently Needed

We cannot keep asking officers to navigate 21st-century threats using 20th-century tools. We cannot expect interagency teams to function with no shared operational language. We cannot continue to turn a blind eye and allow officers to continue to operate “the way it always has been”. And we certainly cannot afford another high-profile failure rooted in miscommunication and lack of collaborative assets.

**Leadership at every level** — Chiefs, prosecutors, sheriffs, state police superintendents and more, must commit to investing in secure, shared, law enforcement-specific communication and collaboration systems. These platforms must be government approved, court compliant, traceable, encrypted, accessible across jurisdictions while at the same time be affordable for agencies and taxpayers.

The tool exists. **The technology is here**. What’s missing is the universal expectation that secure communication and collaboration is the standard, not a luxury. Until we fix that, agencies, leadership and officers will remain exposed, cases will remain vulnerable, and the public we serve will remain at risk. We must **stop reacting to preventable failures** and start building a **smarter, safer, and more connected law enforcement future**.

**Reference Sources:**


- Department of Justice - OIG
- Police Executive Research Forum (PERF)
- WGBH NEWS
- Chicago Tribune
- FBI - CJIS Security Policy
- KTNV.com
- GovTech.com
- OnlinePolicingSolutions.com

# 2025
## Law Enforcement Report

Research and report provided as a law enforcement service from the office of the "National Law Enforcement and Community Policing Integrated Network" (NLECPIN)

# Breaking the Chain of Risk

The Importance of Securing Law Enforcement Communication & Collaboration in the 21st Century

**State of New Jersey**
Report Supplement

**I**n New Jersey, when police officers and agencies use digital communications, such as text messages, mobile app chats, and interagency messaging platforms, to coordinate, plan, discuss, document or manage an investigation or official action, those communications and supporting materials are treated as official law enforcement records and are subject to mandatory preservation and discovery requirements. Attorney General Directive 2010-1 ("Guidelines for the Retention of Evidence") requires that any record or material created or received in the course of an investigation, regardless of format, must be retained according to the Division of Archives and Records Management (DARM) schedules and cannot be destroyed or altered before its scheduled retention period. This includes intra and inter-agency digital communications, operational instructions, collaborative efforts, digital case notes, and any attachments such as images or documents shared electronically.

These requirements stem from both state record-retention laws (N.J.S.A. 47:3-15 et seq.) and the broader duty to preserve information and evidence under criminal procedure and discovery rules. Failing to preserve such communications can constitute spoliation of evidence, which can lead to sanctions, adverse jury instructions, dismissal of charges, civil litigation, internal affairs inquiries and more. In the law enforcement context, the New Jersey Rules of Court (R. 3:13-3) require prosecutors, and by extension, all investigating agencies, to disclose all relevant reports, statements, and records in their possession. If operational directives, communications, plans, investigative updates, or interagency coordination details are exchanged by text or app, they form part of the investigative record and must be stored in an auditable, agency-controlled system.

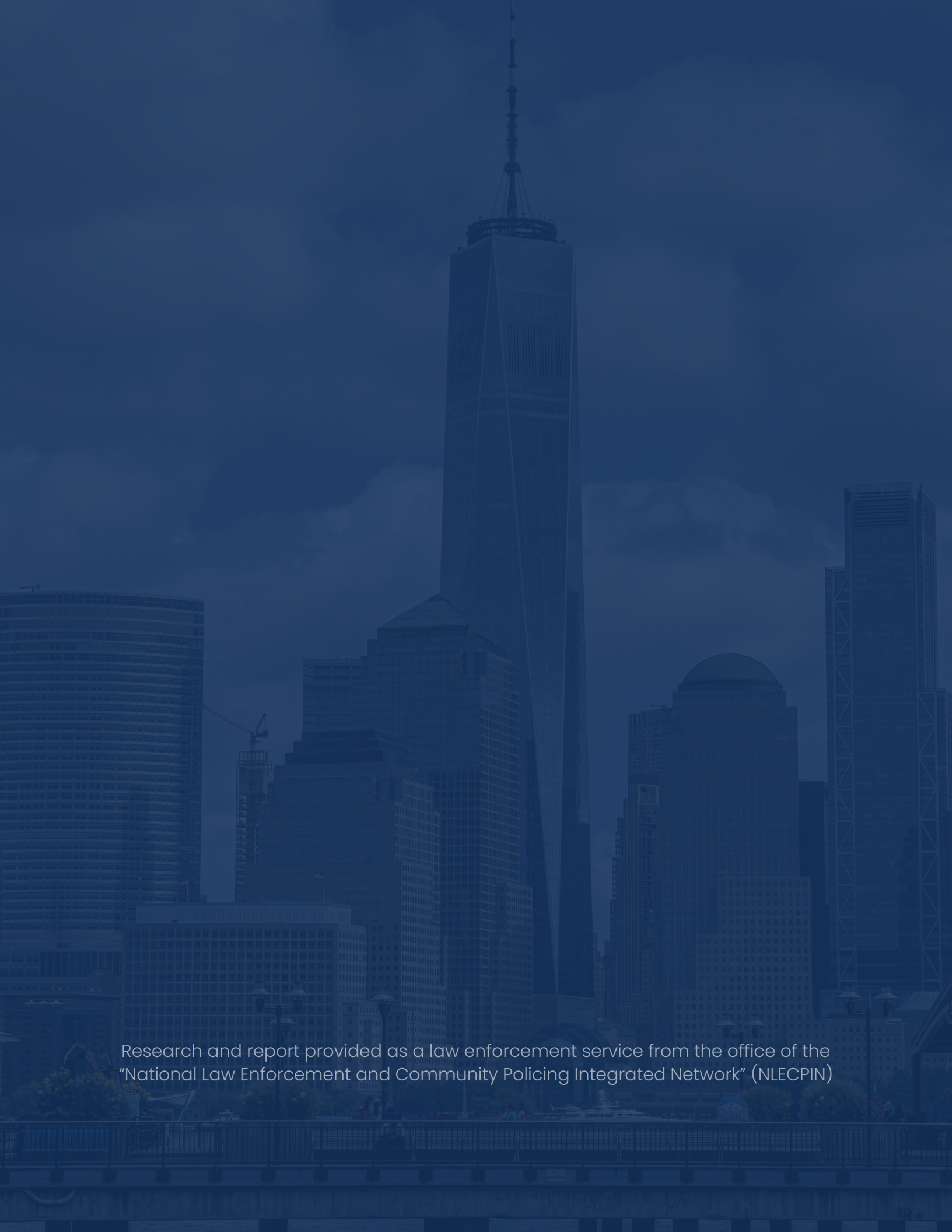
Consumer-grade messaging tools such as Signal, Slack, WhatsApp, or standard SMS texting present a compliance risk because:

- They lack case management features and integration, automatic archiving into a controlled platform, chain-of-custody tracking, and reliable retention controls.
- Many such apps allow for "disappearing" messages or local deletion without central backup, creating gaps in the record and making it impossible to meet Attorney General and DARM preservation requirements. (Some of these "features" may lead to accusations that the law enforcement officers intentionally tried to hide or destroy evidence).
- The absence of a retrievable, authenticated record undermine prosecutions, impede internal reviews, and violate state law.
- These applications are simply NOT developed for official and sensitive law enforcement communications, are handled and controlled differently from user to user, and do not provide any of the required official retention and security requirements that are mandated by the established and ever evolving rules of evidence and record retention.

For these reasons, the New Jersey law enforcement apparatus should only operate on secured, agency-approved platforms that log and preserve actions in compliance with federal and New Jersey law, Attorney General directives, and court discovery obligations.

**Reference Sources:**

- N.J.S.A. 47:3-15 et seq. – Public Records Retention and Disposition Law
- NJ Attorney General Directive 2010-1 – Guidelines for the Retention of Evidence
- NJ Rules of Court, Rule 3:13-3 – Discovery and Inspection in Criminal Matters
- Division of Archives and Records Management (DARM) – Law Enforcement Agency Records Retention Schedules



Research and report provided as a law enforcement service from the office of the
"National Law Enforcement and Community Policing Integrated Network" (NLECPIN)


NATIONAL LAW ENFORCEMENT AND COMMUNITY POLICING INTEGRATED NETWORK