MANAGEMENT ALERT

Oversight Challenges Due to Shared NPSBN Network Architecture

REPORT NO. OIG-26-026-I

AUGUST 24, 2026

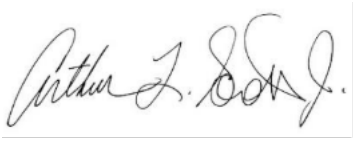
U.S. Department of Commerce
Office of Inspector General
Office of Audit and Evaluation

UNITED STATES DEPARTMENT OF COMMERCE
Office of Inspector General
Office of Audit and Evaluation
Washington, DC 20230

August 24, 2026

MEMORANDUM FOR: Arielle Roth
Assistant Secretary of Commerce for Communications and Information and NTIA Administrator
National Telecommunications and Information Administration

Michael A. Cannon
Executive Director and Chief Executive Officer
First Responder Network Authority



FROM: Arthur L. Scott Jr.
Assistant Inspector General for Audit and Evaluation

SUBJECT: *Management Alert: Oversight Challenges Due to Shared NPSBN Network Architecture*
Report No. OIG-26-026-I

Attached is the final management alert describing the need for independent cybersecurity oversight of the Nationwide Public Safety Broadband Network (NPSBN) and the risks of the current governance structure. This alert results from ongoing work on an evaluation we initiated to assess the effectiveness of NPSBN security controls in detecting and responding to cyber incidents.

We will post the management alert on our website per the Inspector General Act of 1978, as amended (5 U.S.C. §§ 404, 420).

We appreciate your staff's cooperation and professionalism during this evaluation.

Attachment

Introduction

The Nationwide Public Safety Broadband Network (NPSBN) is a nationwide wireless communications network that gives first responders a dedicated, reliable way to communicate when responding to emergencies.[1]

The First Responder Network Authority (FirstNet Authority) was established in 2012 as an independent authority within the National Telecommunications and Information Administration (NTIA) to oversee the building, deployment, and operation of the NPSBN. The establishing law also charges FirstNet Authority with ensuring the safety, security, and resiliency of the network, and includes requirements for protecting and monitoring it to guard against cyberattacks.[2] In March 2017, FirstNet Authority awarded AT&T a $6.5 billion, 25-year contract[3] with a ceiling of $100 billion to deploy the network.[4] The NPSBN was built upon AT&T's commercial network infrastructure, so AT&T owns and operates the NPSBN while FirstNet Authority provides oversight of contractual obligations, among other duties.

The NPSBN is a strategically significant target for advanced cyberattacks. In January 2026, we initiated an evaluation to assess the effectiveness of NPSBN security controls in detecting and responding to cyber incidents. We planned to perform hands-on security testing but were unable to reach an agreement with AT&T to let us conduct independent testing of the NPSBN on the production network or review third-party security tests.

This management alert describes the need for independent cybersecurity oversight of the NPSBN and the risks of the current governance structure.[5]

---

[1] The NPSBN provides a dedicated radio spectrum band for first responders. This band, Band 14, is a spectrum in the 700 MHz band. Public safety users are priority users in Band 14, and commercial users are removed from it when the network is congested.

[2] See Pub. L. No. 112-96, Middle Class Tax Relief and Job Creation Act of 2012, §§ 6204(a) and 6206(b), codified at 47 U.S.C. §§ 1424(a) and 1426(b).

[3] The U.S. Department of the Interior signed the contract on behalf of the U.S. Department of Commerce and FirstNet Authority, then transferred the contract's management to FirstNet Authority in December 2017.

[4] As of December 31, 2023, AT&T had collected over $6.4 billion from FirstNet Authority for activities related to task orders associated with the first 5 years of work, excluding additional reinvestments into the network (according to AT&T's Securities and Exchange Commission filing for calendar year 2023).

[5] On April 27, 2026, we announced a revised evaluation objective that focuses on FirstNet Authority's broader cybersecurity oversight processes. The observations in this management alert are related to our efforts to perform hands-on security testing under the original incident detection and response objective.

Observations

➤ Statutory Basis for Shared Network Architecture

The NPSBN's shared network architecture is rooted in the statutory framework. When Congress created FirstNet Authority in 2012, it required that the network be deployed through a public–private arrangement and leverage existing infrastructure "to the maximum extent economically desirable."[6]

These legislative requirements encouraged an approach in which the selected contractor—AT&T—leveraged its existing nationwide commercial infrastructure rather than building an independent federal network. Consequently, the NPSBN was designed from the outset as a hybrid system, blending dedicated NPSBN components with AT&T's commercial mobile network. This statutory framework directly contributes to the oversight limitations described in this management alert because key operational components reside on private commercial infrastructure. This arrangement significantly restricts opportunities for independent testing and oversight by government entities. Therefore, the statutory design decision inherently shapes the government's ability to conduct independent, hands-on cybersecurity oversight of the NPSBN, even if contractual provisions were to permit such activities.

➤ The NPSBN Is a Target for Advanced Cyberattacks

The NPSBN is a high-value target for advanced cyber adversaries because it underpins critical public safety communications. In 2021, we issued a report produced by The MITRE Corporation about the NPSBN's security architecture.[7] In that report, MITRE states that malicious actors are "continuously developing and deploying tactics and techniques to infiltrate, disrupt, and exploit network activity" and reiterates a warning by the Cybersecurity and Infrastructure Security Agency that cyberspace is "particularly difficult to secure" due to globally distributed threat actors and complex interdependencies.[8]

This broader threat environment now includes groups such as Salt Typhoon, a Chinese state-aligned actor known for targeting critical U.S. infrastructure networks, including communications. Public reporting shows that Salt Typhoon specializes in long-term, stealthy intrusions designed to pre-position themselves inside mission-critical systems for future potential disruption. The NPSBN is especially attractive for this type of infiltration

---

[6] See Pub. L. No. 112-96, § 6206(c)(3).

[7] Commerce OIG, December 14, 2021, *FirstNet Authority Must Increase Governance and Oversight to Ensure NPSBN Security,* OIG-22-011-I.

[8] OIG-22-011-I, iii.

because it underpins nationwide emergency communications, giving adversaries strategic access and potential leverage during a crisis.

As described above, the NPSBN's architecture blends an NPSBN core with AT&T's commercial network infrastructure, creating a shared operational environment. Public safety traffic on the network may traverse both dedicated NPSBN and shared AT&T commercial infrastructure. AT&T retains sole operational control of critical components that the government cannot directly access or test without the contractor's authorization. This interconnected design—absent explicit contractual authorizations—inherently limits the government's ability to perform independent cybersecurity oversight and obtain unfiltered visibility into system behavior.

➤ Oversight Constraints Limit FirstNet Authority's Ability to Ensure the Network Meets Cybersecurity Requirements

FirstNet Authority is responsible for the safety, security, and resiliency of the NPSBN. The establishing law includes requirements for FirstNet Authority to (1) protect and monitor the network to guard against cyberattacks, (2) establish network policies that include technical and operational requirements, as well as practices, procedures, and standards for the management and operation of the network, and (3) conduct ongoing compliance review and monitoring of the management and operation of the NPSBN.[9]

However, because the NPSBN is a contractor-owned and contractor-operated network managed through a service contract, FirstNet Authority does not perform hands-on security testing of the NPSBN. Instead, AT&T retains exclusive control of the shared commercial infrastructure supporting the NPSBN, and FirstNet Authority relies on contractor-performed testing, contractor-provided monitoring data, and contractor reporting to assess compliance with statutory cybersecurity requirements. These structural limitations may reduce FirstNet Authority's ability to independently verify that AT&T is meeting these requirements.

➤ Constraints on Independent Testing Limit OIG's Ability to Independently Verify the NPSBN's Security Posture

Information security controls operate as an interconnected system, influenced by control implementation and human behavior. Document-based reviews evaluate controls in isolation, which may not reveal how controls function together or how human behavior and operational factors influence their effectiveness under real-world attack conditions. In

[9] See 47 U.S.C. §§ 1426(b)(2)(A), 1426(c)(1), and 1426(c)(1)(E).

contrast, hands-on testing provides additional assurance about the effectiveness of controls and, in our experience, identifies weaknesses that may otherwise not be apparent.

As part of planning the evaluation we initiated in January 2026, we conducted a threat assessment and created a plan to perform hands-on testing of the NPSBN that emulated the tactics of Salt Typhoon and other advanced cyber threat actors. Our office has a record of conducting similar hands-on security testing on large, mission-critical systems across the Department of Commerce.

However, we found that, although the NPSBN contract contains audit and inspection provisions, it was unclear whether those mechanisms extended to independent hands-on security testing of the NPSBN. Out of an abundance of caution, because these provisions were not explicit, we attempted to reach agreement with AT&T regarding the scope of our proposed threat emulation testing.

We engaged with AT&T to explore testing options that would address operational concerns while still allowing sufficient independence to evaluate the effectiveness of incident detection and response controls. We were unable to reach agreement that met both parties' needs. AT&T expressed concerns about contractual authorities and the risk that testing might pose to shared NPSBN operations given the network's importance to first responders. As a result, we could not independently conduct the planned threat emulation testing and cannot provide assurance regarding the network's safety, security, and resiliency against tactics of known cyber threat actors. Our inability to independently assess NPSBN security controls through threat emulation testing is evidence of a potential contractual limitation that restricts understanding of the network's cybersecurity posture.[10]

➤ Oversight Challenges Affect FirstNet Authority CORs

FirstNet Authority contracting officer's representatives (CORs) face oversight challenges that parallel those we encountered. Because the NPSBN architecture is intertwined with AT&T's commercial network, CORs have limited to no visibility into the security posture of commercial equipment that processes network data beyond select NPSBN core devices. Consequently, FirstNet Authority CORs lack the independent access needed to validate the security controls protecting the NPSBN. Their oversight is constrained to contractor-supplied information, leaving gaps in assurance regarding the network's safety, security, and resiliency.

[10] See also OIG-22-011-I.

Third-Party Security Tests Are Not Available for Oversight Review

The 2021 MITRE report found that FirstNet Authority "lacks governance over network security and the ability to hold AT&T accountable," noting that it did not have "complete and continuous oversight, monitoring, and visibility into the NPSBN."[11] MITRE found that FirstNet Authority relied heavily on AT&T-provided information, which prevented FirstNet Authority from independently validating AT&T's security performance or confirming timely remediation.[12] This dependence on contractor reporting contributed to what MITRE concluded were "unacceptable levels of risk" across key cybersecurity risk areas.[13]

AT&T provides FirstNet Authority with annual third-party security assessment reports, which we reviewed for this evaluation. A security assessment evaluates controls in isolation, primarily through documentation review and personnel. We found that AT&T's annual reports were insufficient to accomplish our evaluation objective.

However, during our planning phase, we became aware that AT&T engages third parties to perform hands-on security testing on the NPSBN, including penetration testing (i.e., simulated cyberattacks). FirstNet Authority indicated that AT&T is actively exploring what reports or summaries of this testing it may be able to provide to FirstNet Authority. AT&T declined to share these test results with us, citing contractual limitations.

AT&T's position on the matter is consistent with prior reported attempts by other oversight bodies to understand the security posture of the NPSBN. Notably, in February 2022, a Cybersecurity and Infrastructure Security Agency subject matter expert said they had no confidence in the NPSBN's security because they had not been provided results of any cybersecurity audits of the network.[14] More recently, this issue came up again regarding congressional requests for AT&T's response to the Salt Typhoon attacks on nationwide

[11] OIG-22-011-I, iv, 6.

[12] MITRE's 2021 report reflects conditions at the time of its publication. FirstNet Authority took corrective actions to address the report's recommendations. Our current evaluation of FirstNet Authority's cybersecurity governance is under way and will assess whether the present operating environment reflects sustained results from the corrective actions.

[13] OIG-22-011-I, 12.

[14] Wyden, Ron. April 12, 2023. Letter to Cybersecurity and Infrastructure Security Agency Director Jen Easterly and National Security Agency Director Paul M. Nakasone requesting annual cybersecurity audits of FirstNet by the two agencies with results delivered to Congress and the Federal Communications Commission. According to the letter, FirstNet Authority and NTIA said that AT&T obtains independent audits but the Department is unable to share them due to nondisclosure provisions in the NPSBN contract; the letter further notes the agencies said they are "not allowed to reveal how frequently AT&T commissions these audits, how robust they are, what the audit results were, or whether all vulnerabilities discovered during the audits have been fixed."

telecommunication networks.[15] The lack of transparency with respect to security testing reflects an ongoing source of oversight risk.

Conclusion

Constraints on the government's ability to obtain independent access to shared network components limit cybersecurity oversight of the NPSBN.

For example, because critical operational components reside on AT&T-controlled commercial infrastructure, the government cannot:

- Directly observe how security controls operate in practice.
- Independently validate the network's defensive posture.
- Access detailed third-party technical evaluations.

These structural limitations impede both OIG and FirstNet Authority's CORs from performing independent oversight. Strengthening federal visibility into NPSBN cybersecurity will require addressing these architecture-driven barriers, which shape the government's ability to monitor, assess, and enforce security compliance across the network.

Proposed Actions for Change

To address the oversight constraints created by the shared NPSBN architecture, the Department and NTIA should consider taking the following actions:

- Inform congressional stakeholders of the structural oversight limitations and outline potential remedies.
- Engage with AT&T to pursue targeted contractual and technical mechanisms that reduce reliance on contractor-provided information.
- Identify the architectural features that limit federal oversight and develop tailored mitigation strategies.

[15] U.S. Senate Committee on Commerce, Science, and Transportation. February 3, 2026. Press Release, *Cantwell Demands AT&T, Verizon CEOs Come Clean on Salt Typhoon Hacks, Ongoing Network Security Risks*.

These actions would strengthen the federal government's ability to independently assess NPSBN security while preserving the public–private arrangement Congress originally required.

As previously described, our original evaluation objective was to assess the effectiveness of the NPSBN's security controls in detecting and responding to cyber incidents. This management alert is based on fieldwork conducted from January 2026 through April 2026. We are conducting this evaluation in accordance with *Quality Standards for Inspection and Evaluation* (December 2020) issued by the Council of the Inspectors General on Integrity and Efficiency. Those standards require that the evidence must sufficiently and appropriately support evaluation observations and provide a reasonable basis for conclusions related to the objective. We believe that the evidence obtained provides a reasonable basis for our observations and conclusions.

Summary of NTIA's Response

In response to a draft of this management alert, NTIA provided technical comments and comments related to the public releasability of certain statements in the draft. We considered these comments and revised the alert where appropriate.

REPORT

FRAUD & WASTE & ABUSE

HOTLINE

Department of Commerce

Office of Inspector General Hotline

www.oig.doc.gov | 800-424-5197