



NOTICE



Consistent with Section 5274 of the National Defense Authorization Act for Fiscal Year 2023, the Office of Inspector General includes with its reports written responses received within 30 days of publication from nongovernmental organizations or business entities specifically identified in those reports.

This attachment includes any written responses in their entirety. The content of each response is the sole responsibility of the submitting organization, and their inclusion here does not imply our endorsement or agreement. Questions regarding the content of the attached responses should be directed to the respective nongovernmental organization or business entity.

September 24, 2026

Duane Townsend, Acting Inspector General
Office of Inspector General
U.S. Department of Commerce
1401 Constitution Avenue, N.W.
Washington, DC 20230

Re: Management Alert, “Oversight Challenges Due to Shared NPSBN Network Architecture,” Report No. OIG-26-026-I (Aug. 24, 2026)

Dear Acting Inspector General Townsend:

We write in response to the above-referenced Management Alert (the “Alert”). We appreciate the opportunity to provide important context regarding the FirstNet program, its congressionally directed network architecture, and the considerations that must guide cybersecurity oversight of a live telecommunications network.

In brief, we offer four important perspectives:

First, the OIG focuses on oversight structure in the Alert. It **does not** identify a cybersecurity incident, breach, compromise, or network vulnerability; nor does it identify deficiencies in AT&T’s contractual performance. Rather, the OIG seeks threat-emulation testing on a live production network and reviewing certain third-party assessments. While AT&T agrees that effective oversight is important, live-network testing goes well beyond reasonable oversight and raises significant legal, privacy, security, and operational concerns.

Currently, the FirstNet program is subject to extensive public accountability, including oversight by the First Responder Network Authority (FirstNet Authority), its Board, NTIA, Congress, GAO, the Department of Commerce OIG, and the FCC. We respect and welcome that oversight.

However, cybersecurity oversight of a live nationwide telecommunications network must be carefully scoped. AT&T is unaware of any precedent where a federal oversight body has conducted independent adversary-style testing on a privately operated wireless network carrying active customer traffic. Threat-emulation testing simulates hostile cyber activity and, in a live production environment, can cause service degradation, system instability, or interference with legitimate traffic – risks

that are especially consequential for a network supporting first responders and emergency communications.

AT&T has legal and operational responsibilities to safeguard customer information, maintain network integrity, and preserve the reliability of critical communications infrastructure. AT&T continuously tests and monitors its systems through established security, operational, and assessment processes, and, as discussed below, is prepared to engage with FirstNet stakeholders regarding those activities subject to appropriate protections. Accordingly, any government-directed testing or oversight process must be designed to strengthen assurance without introducing new risk to the network or the users it is intended to protect.

Second, the OIG acknowledges that the FirstNet network's shared infrastructure architecture reflects congressional intent: leveraging existing commercial infrastructure to the maximum extent possible to accelerate deployment and support long-term program sustainability. As intended, the FirstNet network combines dedicated public safety assets with shared AT&T infrastructure, delivering nationwide public safety broadband capabilities far more quickly than a stand-alone government-built network could have achieved.

Although the OIG recommends briefing government stakeholders on potential oversight issues related to the FirstNet network's shared infrastructure, that recommendation does not change the fact that this architecture is central – not incidental – to the statutory and contractual framework that enabled FirstNet to meet public safety's need for nationwide reach, reliability, operational resilience, efficient use of limited FirstNet Authority funds, and cybersecurity compliance supported by contractual safeguards and appropriate security controls.

Third, FirstNet is protected by dedicated public safety capabilities and layered cybersecurity safeguards that go beyond standard commercial network cybersecurity measures. FirstNet operates on the nation's only physically separate, dedicated 5G standalone public safety network core, protecting first responders' communications and network performance through quality, priority, and preemption on the network. The network includes firewalls, proxies, intrusion detection systems, access controls, and enhanced security measures, along with a dedicated Security Operations Center providing 24/7 monitoring, threat detection, and incident response. Importantly, FirstNet is reinforced with enhanced measures designed to provide protection without sacrificing usability or impacting public safety's missions.

The FirstNet Authority requires robust cybersecurity compliance, reviewed through weekly, quarterly, and annual oversight processes. AT&T also performs ongoing internal and third-party assessments to meet applicable regulatory, industry, and governance requirements.

Fourth, any access to third-party testing materials must be conditioned on the protection of sensitive security and proprietary information. These reports contain highly sensitive information – including technical findings, methods, tools, and remediation details – that is essential to responsible cybersecurity governance. AT&T will continue working with FirstNet stakeholders to provide meaningful assurance while preserving contractual protections, proprietary information, and operational security.

Public safety's network must remain secure, resilient, and trusted. AT&T is committed to continuously strengthening the FirstNet network's security posture and supports rigorous, outcome-focused oversight that strengthens confidence in the program.

Thank you for your consideration of the above. We welcome the responsibility and accountability that comes with being public safety's network partner, and we will always work with the FirstNet Authority, NTIA, and OIG to provide even better service to America's first responders.

Sincerely,



Scott I. Agnew
President, FirstNet Program at AT&T