FirstNet Authority Must Increase Governance and Oversight to Ensure NPSBN Security

FINAL REPORT NO. OIG-22-011-I

DECEMBER 14, 2021

~~CONTROLLED UNCLASSIFIED INFORMATION~~

~~*Final Report Contains Information Marked*~~
~~**CONTROLLED UNCLASSIFIED INFORMATION**~~

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

UNITED STATES DEPARTMENT OF COMMERCE
Office of Inspector General
Washington, D.C. 20230

December 14, 2021

MEMORANDUM FOR: Edward Parkinson
Chief Executive Officer
First Responder Network Authority

FROM: Frederick J. Meny, Jr.
Assistant Inspector General for Audit and Evaluation

SUBJECT: *FirstNet Authority Must Increase Governance and Oversight to Ensure NPSBN Security*
Final Report No. OIG-22-011-I

Attached is the final report on the evaluation of the Nationwide Public Safety Broadband Network's (NPSBN's) security architecture. The objective was to assess the NPSBN's security risks resulting from its security architecture.

We contracted with The MITRE Corporation (MITRE)—an independent firm—to perform this evaluation. Our office oversaw the progress of this evaluation to ensure that MITRE performed the evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation* (January 2012) and contract terms. However, MITRE is solely responsible for the attached report and conclusions expressed in it.

In its evaluation of the NPSBN security architecture, MITRE identified one overarching finding and three supporting sub-findings:

1. The First Responder Network Authority (FirstNet Authority) lacks governance over network security and the ability to hold AT&T accountable for failing or ineffective security requirements.
    a. Insufficient vulnerability management, specifically patch management and application monitoring processes, leaves the NPSBN more susceptible to exploitation of remote services.
    b. AT&T's Business Continuity Plan/Disaster Recovery Plan has proven ineffective at mitigating and managing some public safety emergency events.
    c. The NPSBN security architecture may be susceptible to supply chain attacks due to FirstNet Authority's inability to validate AT&T's Supply Chain Risk Management.

MITRE recommended that the FirstNet Authority Chief Executive Officer direct the NPSBN Program Management Division staff to take the following actions in coordination with AT&T:

1. Increase governance and ownership over the NPSBN by instituting penalties for failing to meet security requirements (i.e., failing scorecard items).
2. Implement a process to review Critical and High vulnerabilities and mutually agree upon deadlines for remediation within Trade Secret.
3. b(7)(e)
4. Validate the NPSBN Business Continuity Plan/Disaster Recovery Plan by applying lessons learned to first responder-specific continuity scenarios. Use those scenarios to check the underlying assumptions and recovery time requirements and reduce the current recovery time objective and reliance on deployables as an appropriate backup option during a crisis.
5. Develop a comprehensive cyber supply chain risk scoring mechanism and response strategy.
6. Develop an NPSBN-specific supply chain digital roadmap that anticipates future supply chain developments for the purposes of scalability and adaptability.

On September 27, 2021, the Office of Inspector General (OIG) received FirstNet Authority's response to the draft report's findings and recommendations, which is included within the report as appendix G. FirstNet Authority did not concur with the findings but did agree to consult with its expert third-party cybersecurity contractor regarding the recommendations and how to implement the recommendations in an action plan, where appropriate. After considering FirstNet Authority's comments, MITRE upheld and affirmed its findings and recommendations.

Pursuant to Department Administrative Order 213-5, please submit to OIG an action plan that addresses the recommendations in this report within 60 calendar days. This final report will be posted on OIG's website pursuant to sections 4 and 8M of the Inspector General Act of 1978, as amended (5 U.S.C. App., §§ 4 & 8M) unless prohibited from disclosure by law. At the request of FirstNet Authority and AT&T, redactions have been placed in the report and this memorandum to cover sensitive information about IT vulnerabilities that would be protected from release by Exemption 7(E) of the Freedom of Information Act, 5 U.S.C. § 552, and information protected by the Trade Secrets Act, 18 U.S.C. § 1905.

We appreciate the cooperation and courtesies extended to MITRE by your staff during this evaluation. If you have any questions or concerns about this report, please contact me at (202) 482-1931 or Chuck Mitchell, Director for Cybersecurity Audit, at (202) 809-9528.

Attachment

cc: Evelyn Remaley, Acting Assistant Secretary of Commerce for Communications
and Information, NTIA
Lisa Casias, Deputy Chief Executive Officer, FirstNet Authority
Paul Madison, Acting Chief Counsel, FirstNet Authority
John Wobbleton, Senior Director, Policy and Internal Control, FirstNet Authority

Kim Farington, Chief Financial and Administrative Officer, FirstNet Authority
Peggy O'Connor, Director of Program Management, FirstNet Authority
Alice Suh, Senior Analyst, FirstNet Authority
Milton Brown, Deputy Chief Counsel and Audit Liaison, NTIA
Kathy Smith, Alternate Audit Liaison, NTIA
MaryAnn Mausser, Audit Liaison, Office of the Secretary

MTR200159
MITRE TECHNICAL REPORT

Security Evaluation of the Nationwide Public Safety Broadband Network (NPSBN)

for:
Department of Commerce
Office of the Inspector General

FirstNet Authority Must Increase Governance and Oversight to Ensure NPSBN Security.

December 2021

For further information, please contact The MITRE Corporation, Contracts Management Office, 7515 Colshire Drive, McLean, VA 22102-7539, (703) 983-6000.

This page intentionally left blank.

Executive Summary

FirstNet Authority is an independent authority within the National Telecommunications and Information Administration (NTIA) of the Department of Commerce (the Department), with the duty and responsibility to "deploy and operate" the Nationwide Public Safety Broadband Network (NPSBN), a wireless broadband network for first responders.[1] Since 2017, FirstNet Authority has contracted a major U.S.–based telecommunications company, AT&T, to build, operate, and maintain the NPSBN. FirstNet Authority retains contractual responsibility for governance of the NPSBN security architecture.

In September 2020, the Office of the Inspector General (OIG) engaged The MITRE Corporation to assess the NPSBN's security risks resulting from its security architecture. This evaluation's objective includes an assessment of FirstNet Authority's governance of the NPSBN, and of the NPSBN security architecture's effectiveness at mitigating risks and managing threats to this important part of public safety and critical infrastructure.

Why We Did This Review

Cybersecurity is a fast-evolving field with many threats and threat actors continuously developing and deploying tactics and techniques to infiltrate, disrupt, and exploit network activity. According to the federal Cybersecurity and Infrastructure Security Agency (CISA), "Cyberspace is particularly difficult to secure due to a number of factors: the ability of malicious actors to operate from anywhere in the world, the linkages between cyberspace and physical systems, and the difficulty of reducing vulnerabilities and consequences in complex cyber networks." Cyber threats to critical infrastructure, such as the NPSBN, pose a significant risk for "wide scale or high-consequence events" that could harm or disrupt services essential to U.S. economy, businesses, and communities. In this report, MITRE offers recommendations to FirstNet Authority to help protect public safety and critical infrastructure by improving NPSBN operational effectiveness and security.

OIG tasked MITRE with the following overall objective: to assess the NPSBN's security risks resulting from its security architecture. The evaluation included four sub-objectives: (1) identify and document likely threats to the NPSBN; (2) evaluate the current NPSBN security architecture implemented by AT&T against the identified threats, and document the results; (3) identify security risk scenarios resulting from the threat and architecture assessments, including likelihood and impact of occurrence, and map the results to MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) Framework® and the National Institute of Standards and Technology's (NIST) Cyber Security Framework (CSF); and (4) use the resulting risk scenarios and ATT&CK Framework® mapping to generate a report that identifies significant risk groupings and recommends ways to strengthen NPSBN security against those risks.

[1] Middle Class Tax Relief and Job Creation Act of 2012, 26 U.S.C. § 6204 (2012).

What We Found

MITRE conducted its evaluation between November 30, 2020, and March 31, 2021, and identified an overarching finding:

1. FirstNet Authority lacks governance over network security and the ability to hold AT&T accountable for failing or ineffective security requirements.

This overarching finding is supported by three sub-findings:

2. Insufficient vulnerability management, specifically patch management and application monitoring processes, leaves the NPSBN more susceptible to exploitation of remote services.
3. AT&T's Business Continuity Plan/Disaster Recovery Plan (BCP/DRP) has proven ineffective at mitigating and managing some public safety emergency events.
4. The NPSBN security architecture may be susceptible to supply chain attacks due to FirstNet Authority's inability to validate AT&T's Supply Chain Risk Management (SCRM).

What We Recommend

MITRE recommends the FirstNet Authority Chief Executive Officer direct the NPSBN Program Management Division staff to take the following actions in coordination with AT&T:

Table 1. Recommendations

ID	Recommendation	Section
R1	Increase governance and ownership over the NPSBN by instituting penalties for failing to meet security requirements (i.e., failing scorecard items).	2.1
R2	Implement a process to review Critical and High vulnerabilities and mutually agree upon deadlines for remediation within Trade Secret.	2.2
b(7)(e	b(7)(e)	[redacted]
R4	Validate the NPSBN BCP/DRP by applying lessons learned to first responder–specific continuity scenarios. Use those scenarios to check the underlying assumptions and recovery time requirements and reduce the current RTO and reliance on deployables as an appropriate backup option during a crisis.	2.3
R5	Develop a comprehensive cyber supply chain risk scoring mechanism and response strategy.	2.4
R6	Develop an NPSBN-specific supply chain digital roadmap that anticipates future supply chain developments for the purposes of scalability and adaptability.	2.4

Table of Contents

List of Figures

List of Tables

1 Introduction

The Department of Commerce (the Department) Office of the Inspector General (OIG) seeks to improve the efficiency and effectiveness of the Department's programs and operations, and to prevent and detect fraud, waste, and abuse. To support achievement of these goals, OIG's Office of Audit and Evaluation conducts evaluations of the Department's programs and operations. In September 2020, OIG engaged The MITRE Corporation to evaluate the Nationwide Public Safety Broadband Network's (NPSBN) security risks resulting from its security architecture. This evaluation was conducted between November 30, 2020, and March 31, 2021. *See Appendix A for details on this evaluation's scope and methodology.*

1.1 Background

The Middle Class Tax Relief and Job Creation Act of 2012 (the Act) established FirstNet Authority as an independent authority within the National Telecommunications and Information Administration (NTIA), with the duty and responsibility to deploy and operate the Nationwide Public Safety Broadband Network (NPSBN).[2] The NPSBN is intended to provide secure, reliable cellular voice and data communications services for emergency response organizations and personnel, also known as first responders. When the First Responder Network Authority (FirstNet Authority) was established by Congress in February 2012, it was given a clear mission: "ensure the building, deployment, maintenance, improvement, and ongoing operation of a nationwide, interoperable broadband network that helps public safety save lives and protect our nation's communities."[3] The NPSBN is designed for broad use, including public safety events, weather emergencies, natural disasters, and similar occurrences, and is, therefore, an important component of U.S. national, state, and local critical infrastructure.

The NPSBN consists of two primary networks, the core and the radio access network (RAN). The core network provides infrastructure to interconnect the radio network. The RAN allows subscribers to connect their wireless devices to the network throughout the nation. As of October 22, 2020, the NPSBN construction was 80 percent complete, with the following cited accomplishments: 1.7 million+ FirstNet Connections, 14,000+ public safety agencies and organization subscriptions, 150+ apps in the FirstNet App Catalog, 180+ FirstNet Ready Devices, 76+ Dedicated deployable network assets, 2.61 million+ square miles of Long-Term Evolution (LTE) coverage, and 120,000+ square miles of LTE coverage added in 2019.

1.2 FirstNet Authority Ownership and Governance of the NPSBN

FirstNet Authority's mission under public law is to "ensure the safety, security, and resiliency of the network, including requirements for protecting and monitoring the network to protect against cyberattacks." In 2017, FirstNet Authority entered into a 25-year public-private

[2] Middle Class Tax Relief and Job Creation Act of 2012, 26 U.S.C. § 6204 (2012).

[3] Written Testimony of Edward Parkinson before the Subcommittee on Communications, Technology, Innovation, and the Internet Committee on Commerce, Science, and Transportation. United States Senate, September 24, 2020.

partnership with AT&T, a major national telecommunications carrier, to build, operate, and maintain the network. In this public-private partnership, FirstNet Authority maintains governing authority (i.e., oversight, monitoring, and visibility) and ownership over the NPSBN by accepting responsibility for ensuring successful contract execution.

FirstNet Authority uses a scorecard and internal controls to assess whether AT&T is meeting its contractual obligations related to cybersecurity. The scorecard, which was added as a deliverable in a cybersecurity modification to the contract on May 5, 2020, includes 93 requirements to evaluate AT&T on deliverables and the NPSBN's security posture. The scorecard is presented as an Excel sheet and is reviewed twice annually—once as a draft and the second time as a final deliverable. Each requirement is rated on a scale of 0 to 4 (0 is low; 3 is passing; 4 is high). *See Appendix A for details on the cybersecurity requirements outlined in the contract and the scorecard.*

1.3 NPSBN Cybersecurity Architecture Analysis

In conducting this evaluation, MITRE reviewed: (1) the Act, (2) the contract between FirstNet Authority and AT&T, (3) the NPSBN security architecture documents, (4) AT&T's security policies and procedures, (5) AT&T's reporting on the NPSBN's security effectiveness, and (6) the scorecard deliverable. MITRE also interviewed FirstNet Authority and AT&T team members, including the leadership and operations teams from both organizations.

MITRE's analysis began by identifying known threats relevant to the NPSBN—principally, threats to cellular network infrastructure and services. The team analyzed these threats against the known state of security controls and practices used to protect the NPSBN to identify and prioritize which threats were most likely to impact the network. For the NPSBN security architecture analysis, the team used the NIST CSF and related information found on NIST's website to benchmark the NPSBN security architecture's high-level cybersecurity components. *See Appendix B for details on NIST and the CSF.*

MITRE also applied its Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) Framework®, "a globally accessible knowledge base of adversary tactics and techniques based on real-world observations." The ATT&CK Framework® is open-sourced and recognized as an industry best practice and is typically used as a foundation to develop specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.[4] *See Appendix B for details on the ATT&CK Framework®.*

Based on MITRE's findings, analysis of the aforementioned resources, and assessment of the NPSBN's security architecture using the CSF and ATT&CK frameworks, MITRE identified areas of the NPSBN most vulnerable to adversarial attacks and developed generalized "risk scenarios" applying some of the hacking techniques that pose the greatest threats to the NPSBN. These scenarios represent examples of the types of hypothetical situations that could occur and have been used for assessing security risks. *See Appendix A for details on MITRE's methodology for this evaluation.*

[4] The MITRE Corporation. *MITRE ATT&CK Framework* [online].www.attack.mitre.org. (accessed July 26, 2021).

2 Objectives, Findings, and Recommendations

The overall objective of this evaluation was to assess the Nationwide Public Safety Broadband Network's (NPSBN) security risks resulting from its security architecture. The scope of this evaluation includes an assessment of FirstNet Authority's governance of the NPSBN, and of the NPSBN security architecture's effectiveness at mitigating risks and managing threats to this important part of public safety and critical infrastructure. MITRE conducted its evaluation between November 30, 2020, and March 31, 2021.

OIG tasked MITRE with the following four evaluation sub-objectives:

b(7)(e)

2. Evaluate the NPSBN's security architecture implemented by AT&T against the identified threats and document the results (*see Appendix B for details on industry standards and frameworks*).
3. Identify security risk scenarios resulting from the threat and architecture assessments, including likelihood and impact of occurrence, and map the results to MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) Framework® and the National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity, or Cyber Security Framework (CSF) (*see Sections 2.2–2.5 for ATT&CK framework risk scenarios*).
4. Use the mapping of the identified risk scenarios to the ATT&CK and CSF frameworks to generate a report that identifies significant risk groupings and recommends ways to strengthen NPSBN security against those risks (*see Sections 2.1–2.5 for details on MITRE findings and recommendations*).

To answer these objectives MITRE identified the overarching finding that FirstNet Authority lacks governance over network security and the ability to hold AT&T accountable for failing or ineffective security requirements. This finding is supported by three sub-findings:

- Insufficient vulnerability management, specifically patch management and application monitoring processes, leaves the NPSBN more susceptible to exploitation of remote services.
- AT&T's Business Continuity Plan/Disaster Recovery Plan (BCP/DRP) has proven ineffective at mitigating and managing some public safety emergency events.
- The NPSBN security architecture may be susceptible to supply chain attacks due to FirstNet Authority's inability to validate AT&T's Supply Chain Risk Management (SCRM).

The following sections detail MITRE's key observations, findings, and recommendations.

2.1 FirstNet Authority lacks governance over network security and the ability to hold AT&T accountable for failing or ineffective security requirements.

MITRE's evaluation of the NPSBN security architecture revealed the overarching finding that the level of governance FirstNet Authority provides is insufficient to validate the NPSBN security architecture's operational effectiveness *completely and continuously.* By law, as the U.S. government entity responsible for managing the NPSBN service procurement, FirstNet Authority retains contractual accountability for governance of the network's security architecture. NIST's CSF defines the governance role as a key part of every security architecture: "The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements and inform the management of cybersecurity risk."[5] In this report, governance is being used as an "umbrella" term encompassing oversight, monitoring, and visibility. Although FirstNet Authority contracts the operation, build, and maintenance of the NPSBN to AT&T, it is ultimately responsible for ownership of the NPSBN by holding AT&T accountable for operational activities and security requirements that ensure the NPSBN follows the established security architecture design on behalf of intended stakeholders. Since the NPSBN went into production in 2017, FirstNet Authority and AT&T have been unable to leverage internal controls to guarantee the security outcomes necessary to protect the network.[6] As outlined in the security requirements and modifications of FirstNet Authority's contract with AT&T, the scorecard deliverable includes 93 NPSBN requirements related to cybersecurity.[7] Through this evaluation, MITRE observed that although AT&T is reporting the status of these requirements to FirstNet Authority, in some cases AT&T is failing to achieve a passing score on requirements (a 3 out of 4 on the scorecard deliverable detailed below), rendering a requirement ineffective as an internal control to achieve the objective of securing the network on behalf of first responders.

2.1.1 Although the security architecture defines controls, AT&T is not fully complying with contractual security requirements.

MITRE reviewed two scorecards for this report: the scorecard presented by AT&T to FirstNet Authority in July 2020 (submitted as a work in progress for the final annual deliverable for 2020), and the scorecard AT&T presented in March 2021 (in draft format for 2021).[8] In both cases, AT&T did not "pass" the criteria put forward by FirstNet Authority (scorecard requirements are measured on a scale of 0 to 4, with 4 as high and 3 as meeting the FirstNet

[5] NIST, April 2018. *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*, 25.

[6] The Government Accountability Office (GAO) Green Book defines internal controls as "a process used by management to help an entity achieve its objectives." GAO, Standards for Internal Control in the Federal Government. September 2014, GAO-14-704G, 2.

[7] The security requirements listed in the scorecard are not inclusive of all the security requirements listed in the NIST CSF. For more detail on CSF, see Appendix B.

[8] MITRE's fieldwork concluded on March 31, 2021. The final scorecard was not updated until May 2021, therefore, it is out of scope for this evaluation.

Authority standard and thus "passing"). There was marginal improvement in the percent of requirements that failed from July 2020 to March 2021 (in the July 2020 scorecard, b(7)(e) and in March 2021, b(7)(e)). Based on the scorecard from July 2020, the overall rating of the b(7)(e) requirements was b(7)(e), which is below FirstNet Authority's standard of 3.0 as a passing score; b(7)(e)

The table below summarizes the ratings of the specific requirements from the July 2020 scorecard.[10]

Table 2. Overall Scorecard Ratings, July 2020

b(7)(e)	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]		[redacted]	

Source: MITRE Analysis

FirstNet Authority provided feedback to AT&T on specific items from the July 2020 scorecard on August 31, 2020. FirstNet Authority and AT&T agreed on which scorecard items should be prioritized for resolution; these mutually agreed upon items are referred to as "Big Rocks." AT&T presented updates on the Big Rock items to FirstNet Authority during meetings on November 12, 2020, January 14, 2021, and February 26, 2021.

MITRE analysis found that although AT&T made some improvements to Big Rocks since August of 2020, there was little consistency in how the improvements were applied to the scorecard as described in AT&T's presentations. AT&T did not disclose in the presentations if the Big Rocks had eventually been improved to meet FirstNet Authority's standards. MITRE found no evidence that FirstNet Authority is holding AT&T accountable for failing to fix the requirements. Additionally, the contract currently does not include penalties to hold AT&T accountable for failing security requirements listed in cybersecurity sections of the contract.

[9] In the July 2020 Scorecard, one item was not scored. The total number of requirements in the table is [redacted], because it does not include the one item that was not scored.

[10] The final version of the 2021 scorecard was not complete as of the end of fieldwork (March 31, 2021).

FirstNet Authority's inability to hold AT&T accountable for failing or ineffective scorecard requirements demonstrates insufficient governance. Furthermore, FirstNet Authority lacks complete and continuous oversight, monitoring, and visibility into the NPSBN, resulting in a failure to guarantee the network's operational effectiveness. This leaves the NPSBN susceptible to higher levels of "unacceptable"[11] risk by threat actors, an ever-present and significant risk to critical infrastructure.

2.1.2 Recommendation

To address this finding, MITRE recommends the FirstNet Authority Chief Executive Officer direct the NPSBN Program Management Division staff to take the following actions in coordination with AT&T:

R1: Increase governance and ownership over the NPSBN by instituting penalties for failing to meet security requirements (i.e., failing scorecard items).
The following sections support this overarching finding—they address three areas that pose significant risks to the NPSBN based upon conclusions from this evaluation.

2.2 Insufficient vulnerability management, specifically patch management and application monitoring processes, leaves the NPSBN more susceptible to exploitation of remote services.

Vulnerability management is a risk-based, established, and continuous process designed to address the need to identify and remediate threat vulnerabilities. Cybersecurity threats exist when a threat actor can exploit an outstanding vulnerability. Threats can lead to an undesired event with negative consequences to the network, critical infrastructure, and public safety. Common threats are data loss or theft, including the loss of sensitive records, citizens' personal information, law enforcement data, critical infrastructure information, healthcare data, and dispatch information and legal liability for the parties responsible for protecting the systems and the data.

According to AT&T's statements in quarterly project management reviews (PMR), security architecture update meetings with FirstNet Authority, AT&T is continuing to mature its vulnerability management process. However, MITRE found AT&T's current vulnerability management process deficient in two primary areas: patch management and application monitoring.

[11] Risk levels should be agreed to by FirstNet Authority and AT&T, but in general unacceptable risk is any action or lack thereof that increases the statistical probability of a cyberattack occurring that either disrupts or stops a service.

2.2.1 FirstNet Authority is not holding AT&T accountable for deficiencies in the patch management process.

To prevent cyberattacks, organizations that follow cybersecurity industry standards incorporate into their vulnerability management process a continuous[12] scan of their assets. Scan results show security holes in the systems, generally categorized as Critical, High, Medium, and Low. Based on the security hole and its category, application and hardware vendors make patches[13] available to apply to the affected systems to repair susceptible areas. While systems are awaiting vendor-provided patches, threat actors use different techniques to deploy malware, modify system files to their benefit, and lock files, potentially rendering systems unusable. Therefore, patches should be applied to Critical and High categories as soon as possible, typically within the industry standard of 30 to 60 days.

Through this evaluation, MITRE found AT&T had recently improved scanning to take place every b(7)(e) Although AT&T documented that it had adopted the Trade Secret In some instances, AT&T was taking b(7)(e) to patch vulnerabilities. In the PMR on February 26, 2021, AT&T's aggregate quarterly vulnerability data indicated there were b(7)(e) of outstanding b(7)(e) b(7)(e) vulnerabilities leave the system susceptible to potential exploits.

AT&T shares *aggregated quarterly scan results* (total vulnerabilities outstanding, vulnerabilities remediated in the last quarter, and plan to remediate remaining vulnerabilities in the next quarter) with FirstNet Authority in their quarterly PMR, at which time some vulnerabilities had been open for more than Trade Secret Because these updates are quarterly, FirstNet Authority cannot ensure remediation within Trade Secret leaving the NPSBN more susceptible to risk. The review of quarterly aggregate results is not sufficient from a security oversight perspective since FirstNet Authority may not be aware of vulnerabilities that have been open for over Trade Secret

2.2.2 FirstNet Authority lacks insight into the application monitoring process.

b(7)(e)

[12] Center for Internet Security, July 2019, *CIS Controls v7.1 and Sub-Controls Mapping to ISO 27001*. Washington, DC. Line 30 – 31.

[13] "Patches are software and operating system (OS) updates that address security vulnerabilities within a program or product. Software vendors may choose to release updates to fix performance bugs, as well as to provide enhanced security features." CISA, July 2009. CISA. Understanding Patches and Software Updates [online]. www//us-cert.cisa.gov/ncas/tips/ST04-006 (accessed August 3, 2021).

b(7)(e)

[redacted]

[redacted]

[redacted]

2.2.3 The vulnerability management risk scenario highlights possible security risks to the NPSBN b(7)(e).

Threat actors could b(7)(e) systems b(7)(e) are susceptible to exploits; common threats include deploying malware, taking ownership of the systems' files, stealing passwords, and stealing data. b(7)(e)

b(7)(e)

b(7 b(7)(e)

b b(7)(e)

b b(7)(e)

b(7)(e)

2.2.4 Recommendations

To address this finding, MITRE recommends the FirstNet Authority Chief Executive Officer direct the NPSBN Program Management Division staff to take the following actions in coordination with AT&T:

> **R2:** Implement a process to review Critical and High vulnerabilities and mutually agree upon deadlines for remediation within Trade Secret
>
> b(7)(e)

2.3 AT&T's Business Continuity Plan/Disaster Recovery Plan (BCP/DRP) has proven ineffective at mitigating and managing some public safety emergency events.

Effective contingency planning minimizes the impact of natural and man-made disasters that can disrupt the operation of an information system and mission-critical functions.[19] Two common types of contingency plans are the Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP).[20] According to NIST, continuity plans should be developed to provide interoperable communication and continuity of key business operations with essential suppliers, or other agencies, until normal operation can be resumed. Continuity plans should identify incremental strategic or procedural changes and any gaps in capabilities that need to be addressed.

AT&T has demonstrated the importance of contingency planning in its documents shared with FirstNet Authority and in their annual and quarterly meetings. Although AT&T has implemented a comprehensive Business Continuity Management process, these plans have been unsuccessful at mitigating and managing some public safety events, such as the Nashville incident on December 25, 2020.

b(7)(e)

b(7)(e)

[19] NIST, May 2010. *Special Publication 800-34: Contingency Planning Guide for Federal Information Systems*. 5.

[20] NIST, May 2010. *Special Publication 800-34: Contingency Planning Guide for Federal Information Systems*.11.

2.3.1 In the Nashville Incident, AT&T’s BRP/DCP failed to maintain the operational purpose of the network.

The NPSBN was designed for first responders to be a resilient, redundant, reliable, and self-healing infrastructure with continuous operation[21] in the event of a disaster or catastrophe. However, in the case of the Nashville incident, AT&T’s BCP and DRP procedures proved ineffective at providing uninterrupted, continuous operation of the NPSBN service. During the Nashville incident:

- The NPSBN service was disrupted due to a bombing that caused AT&T’s building to lose power (backup batteries provided service for a few hours). An alternate source of power also failed due to flooding.
- AT&T did not incorporate remote recovery options into any response scenario to initiate progress while direct access was not available.
- The NPSBN service was disrupted across the region for 3 to 4 hours during a public safety emergency.

One area of weakness in AT&T’s BCP/DRP highlighted during the Nashville incident was an ineffective recovery time objective (RTO).[22] The FirstNet Authority and AT&T’s contract stipulates an RTO of up to 14 hours. The information provided to MITRE did not demonstrate why 14 hours was determined to be a justifiable RTO; MITRE concluded that the recovery time of 14 or more hours does not align with the NPSBN’s operational purpose.

As stated above, the NPSBN service was disrupted during the Nashville incident for 3 to 4 hours after all backup options were exhausted. Although this recovery window was below the 14-hour RTO described in AT&T’s continuity plan, an RTO of 14 hours is high, and potentially unacceptable, for a mission-critical network that is part of our nation’s critical infrastructure. With the understanding that it is impossible to predict every possible public safety emergency, considering similar public safety scenarios during initial BCP/DRP planning could lead to reduced recovery times in the future.

A second area of weakness in AT&T’s BCP/DRP was a high reliance on deployable (mobile) units to supplement NPSBN service. Although deployables functioned as intended in the Nashville incident by temporarily restoring network communications after about 4 hours (under the 14 hours of RTO stated in the contract), they were insufficient from a public safety and security perspective, as first responders were unable to rely on the NPSBN for 3-4 hours while responding to the crisis.

[21] FirstNet, March 2021. *Security Appendix V20210331 (FirstNet Security Reference Guide)*.215.34, 36, 37 and 38.

[22] “RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources.” Higher RTO (in hours) means it is acceptable for the systems to be unavailable for a longer period of time. RTO is an important number to use in creating the BCP/DRP to minimize impact on service. NIST, May 2010. *Special Publication 800-34: Contingency Planning Guide for Federal Information Systems*.11. 17.

In an initial draft of the document in February 2021 and in a presentation to FirstNet Authority in March 2021, AT&T communicated its findings about the Nashville incident to FirstNet Authority in a detailed After Action Report (AAR)[23] that focused on service restoration for the AT&T commercial network and impact to the NPSBN.[24] AT&T noted in the AAR how it intends to reduce the risk of future events and ensure its processes, network, and infrastructure are more resilient going forward. However, AT&T did not disclose plans to address the significant finding that it relies heavily on deployables, which pose a risk as a primary source of backup. Considering the significance of deployables to NPSBN recovery and the public accessibility of their specifications, deployables could be a target for a malicious actor during service restoration, bringing the effectiveness of the continuity plan into question. The following hypothetical risk scenario demonstrates how a threat actor could exploit a lengthy RTO and reliance on deployable units as the primary network recovery option.

2.3.2 The BCP/DRP risk scenario highlights possible security risks to the NPSBN via deployable exploitation.

Although the deployables backup option functioned as designed in the Nashville incident (after 3 to 4 hours), this may not be the case in the future if sophisticated threat actors impact deployables' operability and integrity. Consequently, future events could have a greater likelihood of disrupting first responders' access to the network, impacting telecom operations and critical infrastructure, putting public safety at risk.

When a BCP/DRP has an RTO of 14 hours and reliance on deployables, there is a significant window in which the deployables could be exploited to prevent restoration of the NPSBN. MITRE analysis showed no indication that FirstNet Authority has any oversight or security requirements for these deployable units to ensure efficacy in the face of hostility or resistance, or for their level of security and integrity. b(7)(e)

2.3.3 Recommendation

To address this finding, MITRE recommends the FirstNet Authority Chief Executive Officer direct the NPSBN Program Management Division staff to take the following actions in coordination with AT&T:

> **R4:** Validate the NPSBN BCP/DRP by applying lessons learned to first responder–specific continuity scenarios. Use those scenarios to check the underlying assumptions and recovery time requirements and reduce the current RTO and reliance on deployables as an appropriate backup option during a crisis.

[23] After Action Reports are a tool to capture lessons learned and best practices after an incident.

[24] The AAR is not publicly available.

2.4 The NPSBN security architecture may be susceptible to supply chain attacks due to FirstNet Authority's inability to validate AT&T's Supply Chain Risk Management (SCRM).

Global trends indicate supply chain risk management is becoming one of the most prevalent areas of cybersecurity vulnerability. The increasing volume and scale of supply chain compromises and rapid advancement of technology makes standardizing a Supply Chain Risk Management (SCRM) practice crucial for organizations to protect against current supply chain threats and prepare for the future.[25][26] An effective method for measuring supply chain risk is to complete a supply chain risk assessment, ensuring expediency and alignment across internal stakeholders. Although AT&T has an SCRM policy, there is a significant disconnect in communication between AT&T and FirstNet Authority regarding supply chain processes and supply chain risk acceptance.

2.4.1 Ineffective communication between FirstNet Authority and AT&T increases unacceptable supply chain risk.

FirstNet Authority does not have a systematic process for validating the NPSBN's cyber supply chain risk exposures, threats, and vulnerabilities, resulting in unacceptable levels of risk; unacceptable risk is any action, or lack thereof, that increases the statistical probability of a cyberattack occurring that either disrupts or stops a service. Although acceptable risk levels should be agreed to by FirstNet Authority and AT&T to ensure alignment in the event of a crisis, MITRE did not find evidence of regular communications regarding supply chain risk and vulnerabilities. There are also no specific contractual requirements pertaining to acceptable levels of supply chain risk or a mutually agreed upon supply chain risk acceptance process.

According to the documents FirstNet Authority and AT&T provided to MITRE, and insight gathered from interviews with both parties, FirstNet Authority *can request supply chain information* directly from AT&T to perform a supply chain risk assessment. However, between when the NPSBN went into production in 2017[27] and the time of this evaluation, FirstNet Authority had not performed a supply chain risk assessment of AT&T's SCRM as it applies to the NPSBN. Consequently, FirstNet Authority has limited visibility into the NPSBN supply chain and is not fully aware of the level of risk it has taken on. The impact is that in the event of an incident, FirstNet Authority may be unable to hold AT&T accountable for a supply chain

[25] Office of the Director of National Intelligence, April 2021, *Annual Threat Assessment of the US Intelligence Community.*[15, 21]

[26] Homeland Security, October 2020, *Homeland Threat Assessment.*[15]

[27] GAO. January 2020. *PUBLIC-SAFETY BROADBAND NETWORK: Network Deployment Is Progressing, but FirstNet Could Strengthen Its Oversight*.7.

exploitation.[28] [29] The following hypothetical risk scenario demonstrates how a threat actor could exploit this lapse in communication to affect the NPSBN.

2.4.2 The Supply Chain Risk Management scenario highlights possible security risks via an AT&T equipment supplier.

Supply chains can be compromised in a multitude of ways. One example would be an incident at a facility of an important AT&T equipment supplier. In this instance, the supplier would be compromised and allow an infected device to enter the NPSBN's supply chain production line; this compromise would be in addition to over a dozen other security incidents in the last year. The specifics of each occurrence would have been reported to the security management team at AT&T. While AT&T could have accepted the risk of working with a supplier with a history of security compromises, it might not have communicated this risk acceptance to FirstNet Authority, nor a course of action with a mutually agreed upon schedule to remediate the issues with the supplier. Consequently, FirstNet Authority would potentially be unaware of the magnitude of risks it is accepting in using this supplier to support the NPSBN.

2.4.3 Recommendations

To address this finding, MITRE recommends the FirstNet Authority Chief Executive Officer direct the NPSBN Program Management Division staff to take the following actions in coordination with AT&T:

> **R5.** Develop a comprehensive cyber supply chain risk scoring mechanism and response strategy.
>
> **R6.** Develop an NPSBN-specific supply chain digital roadmap that anticipates future supply chain developments for the purposes of scalability and adaptability.

3 Conclusion

During this evaluation, MITRE found that FirstNet Authority's security requirements and governance (i.e., visibility, oversight, and monitoring) over the NPSBN should be strengthened for more effective risk management. MITRE's analysis, including analysis of the scorecard deliverable, revealed unacceptable levels of risk in the areas of Vulnerability Management, Business Continuity/Disaster Recovery, and Supply Chain Risk Management.[30] MITRE based these findings on a thorough study of the provided system documentation and data, interviews, publicly available information, and application of the NIST CSF and MITRE ATT&CK frameworks.

[28] AT&T provides an annual Critical Design Security Appendix (CDSA) update, it is loosely structured and not necessarily a systematic examination of the NPSBN's cyber supply chain risks, likelihood of occurrence, and potential impacts.

[29] AT&T is ISO9001 certified

[30] Risk levels should be agreed to by FirstNet Authority and AT&T, but in general unacceptable risk is any action or lack thereof that increases the statistical probability of a cyberattack occurring that either disrupts or stops a service.

MITRE concluded that since the NPSBN went into production in 2017, FirstNet Authority and AT&T have been unable to leverage internal controls to guarantee the security outcomes necessary to protect the network. There is a distinction between AT&T's and FirstNet

Authority's roles and responsibilities regarding the overall security of the NPSBN. Although FirstNet Authority contracts the build, maintenance, and operation of the NPSBN to AT&T, it retains contractual accountability for governance of the security architecture. Increased FirstNet Authority governance of the NPSBN security architecture would help lower the risk of network exploitation by threat actors.

4 Summary of Recommendations

To address the findings in the report, MITRE recommends that the FirstNet Authority Chief Executive Officer direct the NPSBN Program Management Division staff to take the following actions in coordination with AT&T:

R1: Increase governance and ownership over the NPSBN by instituting penalties for failing to meet security requirements (i.e., failing scorecard items).
R2: Implement a process to review Critical and High vulnerabilities and mutually agree upon deadlines for remediation within Trade Secret b(7)(e)

R4: Validate the NPSBN BCP/DRP by applying lessons learned to first responder–specific continuity scenarios. Use those scenarios to check the underlying assumptions and recovery time requirements and reduce the current RTO and reliance on deployables as an appropriate backup option during a crisis.
R5. Develop a comprehensive cyber supply chain risk scoring mechanism and response strategy.
R6. Develop an NPSBN-specific supply chain digital roadmap that anticipates future supply chain developments for the purposes of scalability and adaptability.

5 Summary of Agency Response and MITRE Comments

MITRE received FirstNet Authority's response to the draft of this report on September 27, 2021. FirstNet Authority did not concur with the findings but did agree to consult with its expert third party cybersecurity contractor regarding the recommendations and how to implement the recommendations in an action plan, where appropriate.

After considering FirstNet Authority's comments, MITRE upholds and affirms the fidelity of its findings and recommendations. The purpose of the evaluation was to assess NPSBN security risks resulting from its security architecture. The evaluation period was November 30, 2020 – March 31, 2021. MITRE reviewed documentation provided by FirstNet Authority during the evaluation period and identified findings based on the data, information, and trends in the documentation against industry standards, as well as interviews with FirstNet Authority and AT&T personnel. Subsequent to the evaluation period, FirstNet Authority provided additional documents, which were reviewed as appropriate. MITRE affirms that new information provided did not change the findings or recommendations.

MITRE summarized FirstNet Authority's response to each finding and recommendation and provided comments within this section of the report.

In response to Finding #1:

- FirstNet Authority states that the finding is not accurate because "AT&T provides scores of artifacts to the FirstNet Authority…that allows the FirstNet Authority to provide ample oversight." MITRE reviewed the documents provided by FirstNet Authority during the evaluation and affirms the finding.

- FirstNet Authority states that "as of the close of this report, the scorecard was still a work in progress, and these scores were not the final scores, and have improved." The draft report was updated to reflect that the two scorecards were received as interim deliverables. Subsequent to the period of evaluation, MITRE received and reviewed the final scorecard (dated May 10, 2021). b(7)(e)

In response to Finding #2:

- FirstNet Authority notes that the report "conflates vulnerability management of applications supporting the infrastructure of the network with vulnerability management of third-party mobile applications downloaded by subscribers and running independently on subscriber user equipment." In this regard, FirstNet Authority is mistaken. The report includes a separate finding and recommendation for vulnerability management and application monitoring. Sections 2.2.1 and 2.2.2 of the report cover each topic separately.

- FirstNet Authority alleges that references in the report to "vulnerability numbers are outdated…which would leave a reader with an inaccurate impression of the vulnerability profile of the NPSBN." MITRE affirms the information provided by FirstNet Authority was current and accurate during the period of the evaluation and reflected the vulnerability profile of the NPSBN at the time.

In response to Finding #3:

- FirstNet Authority states that the "discussion of the Nashville bombing is not relevant to MITRE's mandate of conducting a cybersecurity review". The Nashville bombing is an example of the NPSBN not being available for use during a critical public safety event. Business Continuity and Disaster Recovery are important parts of cybersecurity and security architecture, and thus were included in the review. In the report, MITRE recommends that FirstNet Authority review AT&T's Business Continuity and Disaster

- Recovery planning processes and the lessons learned from this outage to minimize any future outages.

- FirstNet Authority states that the length of the outage is incorrect. The report was updated to include FirstNet Authority's technical comments about the length of the outage.

In response to Finding #4:

- FirstNet Authority notes that "the Government is not purchasing devices or assets from the contractor…[and] it is AT&T's responsibility to test, implement, and operate devices and software supplied by its vendors." While FirstNet Authority describes AT&T's practices, MITRE did not make claims regarding AT&T's supply chain practices. Instead, the report is focused on FirstNet Authority as the U.S. government entity responsible for managing the NPSBN service procurement and contractual accountability for governance of the network's security architecture.

- FirstNet Authority notes that AT&T is ISO 27001 and 9001 certified and that FirstNet Authority is purchasing a service, neither of which exempts FirstNet Authority from its
- governmental responsibility to ensure the NPSBN's safety from a Supply Chain Risk Management perspective.

MITRE appreciates the courtesies extended by FirstNet Authority and AT&T personnel during the course of this evaluation.

Appendix A Objectives, Scope, and Methodology

MITRE conducted this evaluation in accordance with the *Quality Standards for Inspection and Evaluation (2011 Edition, January 2012.)*[31][32] MITRE believes that the evidence obtained through this evaluation delivers a reasonable basis for its findings and conclusions based on the review objectives. The Office of the Inspector General (OIG) provided oversight to ensure the work was completed in compliance with the Council of the Inspectors General on Integrity and Efficiency guidance.

A.1 Objectives

The overall objective of this evaluation was to assess the Nationwide Public Safety Broadband Network (NPSBN) security risks resulting from its security architecture. The overall objective was broken down into four sub-objectives:

- **Objective 1. Threats and Vulnerabilities:** *What are the likely threat actors, threats, and vulnerabilities to the NPSBN's security?* Identify and document likely threat actors, threats, and vulnerabilities.
- **Objective 2. Threats and Vulnerabilities Associated with the Security Architecture:** *What are the threats and vulnerabilities associated with the security architecture?* MITRE analysis included reviewing the NPSBN security architecture (core network and radio network) and the Security Reference Guide (also known as the Critical Design Security Annex [CDSA]).
- **Objective 3. Security Risk Scenarios:** *What are the risk scenarios (including likelihood and impact of occurrence) that result from the identified threats, threat actors, and vulnerabilities?*
- **Objective 4. Recommendations to strengthen the security of the NPSBN:** *What are the recommendations associated with the first three objectives?*

A.2 Scope

The scope of this evaluation includes an assessment of FirstNet Authority's governance of the NPSBN, and of the NPSBN security architecture's effectiveness at mitigating risks and managing threats to an important part of public safety and critical infrastructure.

The evaluation was a paper-based evaluation that is a "snapshot in time," which included review of documents dated up to and including March 31, 2021. The evaluation included, but

[31] The *Quality Standards for Inspection and Evaluation* was updated in December 2020 but was out of scope for consideration in this evaluation.

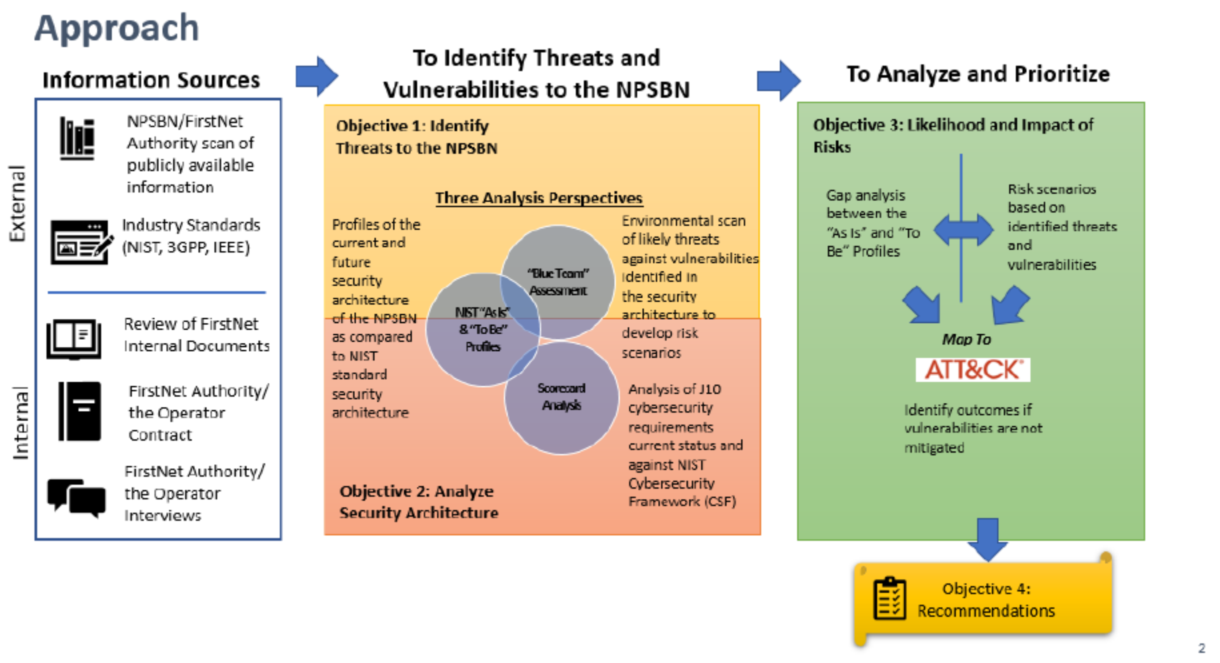
[32] CIGIE. Quality Standards for Inspection and Evaluation (2011 Edition), January 2012. 1.

was not limited to, the cybersecurity requirements in the contract between AT&T and FirstNet Authority, the CDSA, and industry best practices.

A.3 Methodology

Figure 1 below shows how MITRE's analyses align with the objectives.

Figure 1. Evaluation Approach



Approach

Information Sources

External

NPSBN/FirstNet Authority scan of publicly available information

Industry Standards (NIST, 3GPP, IEEE)

Internal

Review of FirstNet Internal Documents

FirstNet Authority/ the Operator Contract

FirstNet Authority/ the Operator Interviews

To Identify Threats and Vulnerabilities to the NPSBN

Objective 1: Identify Threats to the NPSBN

Three Analysis Perspectives

Profiles of the current and future security architecture of the NPSBN as compared to NIST standard security architecture

NIST "As Is" & "To Be" Profiles

"Blue Team" Assessment

Scorecard Analysis

Environmental scan of likely threats against vulnerabilities identified in the security architecture to develop risk scenarios

Analysis of J10 cybersecurity requirements current status and against NIST Cybersecurity Framework (CSF)

Objective 2: Analyze Security Architecture

To Analyze and Prioritize

Objective 3: Likelihood and Impact of Risks

Gap analysis between the "As Is" and "To Be" Profiles

Risk scenarios based on identified threats and vulnerabilities

Map To

ATT&CK

Identify outcomes if vulnerabilities are not mitigated

Objective 4: Recommendations

2

Source: MITRE

In Figure 1, the Information Sources section highlights the external and internal documents MITRE reviewed. The external documents are publicly available and included industry standards. The internal documents include the contract, architecture documents, and interviews.

The middle section of the graphic shows how the team's three analytic perspectives align to Objective 1 and 2.

- **The NIST "As Is" and "To Be" Profiles:** MITRE leveraged the NIST Cyber Security Framework (CSF) to create profiles of the current and future architecture. The profiles represent an alignment of cybersecurity requirements with engineering and operational methodologies. The team's analysis describes how the CSF can be used to represent the current and recommended future states of the NPSBN, and explains the processes and information used to express NPSBN security architecture views derived from written and verbal information from multiple sources. Current and future (i.e., As Is and To Be) views of the security architecture were used to demonstrate the NPSBN security architecture as envisioned and implemented by AT&T, and to demonstrate whether the architecture conforms to accepted best commercial practices expressed in the CSF. MITRE reviewed the NPSBN security architecture and associated cybersecurity threats and risks. MITRE's analysis included reviewing publicly available documents, documents provided by AT&T, and the contract between AT&T and FirstNet Authority and conducting interviews with FirstNet Authority and AT&T staff to provide information that may not be available in the documentation.

- **The "Blue Team" Assessment:** MITRE's analysis includes mapping the threats, threat actors, and vulnerabilities to the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) Framework® and the NIST CSF. It also includes a "Blue Team" approach to identify how known vulnerabilities could impact the NPSBN. "Blue Teams" typically work in conjunction with "Red Teams." Red team–blue team exercises take their name from their military antecedents. The idea is simple: one group of security pros—a red team—attacks something, and an opposing group—the blue team— defends it.[33] MITRE's use of Blue Team began by identifying known threats that are relevant to FirstNet Authority—principally, threats to cellular network infrastructure and services. The Blue Team analyzed these threats against the known state of security controls and practices used to protect the NPSBN to identify and prioritize the threats most likely to impact NPSBN security.
- **The Scorecard Analysis:** MITRE's analysis includes how well the scorecard mapped to the cybersecurity section of the contract, how well AT&T performed on the scorecard, vulnerabilities associated with low-scoring requirements, and how well the scorecard measures the NPSBN security (specifically, how the scorecard mapped to NIST CSF). The third box in Figure 1 shows how the perspectives feed into the analysis and prioritization of risk scenarios. MITRE created risk scenarios based on the gaps between the "As Is" and "To Be" profiles and identified threats and vulnerabilities. MITRE mapped those risk scenarios to the MITRE ATT&CK Framework® and identified techniques the NPSBN *could be vulnerable to*, and *outcomes if those vulnerabilities are not mitigated*. The MITRE ATT&CK Framework® is a publicly available collection of cyber adversary techniques, tactics, and procedures (TTPs) and a knowledge base of observed real-world adversary behavior. It helps identify tactics and techniques the specified infrastructure is vulnerable to, and it provides real-world examples of these tactics and techniques in use and possible ways to detect and mitigate them. MITRE ATT&CK can be used to identify technical and/or procedural mitigations for residual risks to the specified infrastructure.[34] MITRE compiled the information from these perspectives and the analyses to make recommendations.

[33] Red team versus blue team: How to run an effective simulation [online].www.csoonline.com/article/2122440/emergency-preparedness-red-team-versus-blue-team-how-to-run-an-effective-simulation.html (accessed July 26, 2021.)

[34] The MITRE Corporation. *MITRE ATT&CK Framework*.www.attack.mitre.org [online]. (accessed July 26, 2021).

A.3.1 Research

The Research Phase of the project included reviews of publicly available documents, best practices, and documents shared by FirstNet Authority and AT&T. MITRE also conducted interviews with leadership and technical teams from FirstNet Authority and AT&T.

A.3.2 Document Review

MITRE reviewed publicly available information to support the evaluation and to get general information and status updates. These included:

- The Middle Class Tax Relief and Job Creation Act of 2012, which established FirstNet Authority and the NPSBN
- OIG Reports, GAO Reports, and Reports to Congress specific to FirstNet Authority
- Literature: journal articles, magazine articles, public discussions, intellectual property–related news feeds, publicly available reports and analyses, legislative histories, security vendor publications, etc.
- Industry standards that MITRE used to evaluate the NPSBN security architecture, including:
    - NIST CSF
    - NIST 800-53
    - ISO 27001
    - SANS Institute Publications
    - CIS Security Controls
    - ENISA Reports
    - MITRE ATT&CK
    - Institute Electrical and Electronics Engineers (IEEE) Publications

MITRE reviewed FirstNet Authority and AT&T internal and public released documents specifically related to the security architecture. These included:

- The Request for Proposal (RFP) for an Operator of the NPSBN
- The contract between FirstNet Authority and AT&T
- The proposal that AT&T submitted to FirstNet Authority
- NPSBN Documentation: Architecture, Functionality, Security Controls, Critical Design Security Annex (CDSA), Quarterly Program Management Reviews, and Annual Security Reviews
- Scorecard

A.3.3 Interviews

MITRE conducted a series of interviews with leadership and technical teams from FirstNet Authority and AT&T. The purpose of the interviews was to validate, clarify, and obtain additional insights on the documents MITRE received. For the interviews, MITRE created an interview guide, developed standard questions, tailored questions to the roles, and submitted notes from the interviews.

The roles of the FirstNet Authority interviewees included:

- CEO and Deputy CEO
- Chief Network and Technology Officer
- Chief Financial and Administrative Officer
- Senior Director of Roadmap Development
- Chief Counsel and Deputy Chief Counsel
- Deputy Chief Network and Technology Officer
- Direct of Program Management
- Senior Manager, Network Cyber Security
- Senior Cyber Security Engineer
- Senior Manager, Network Technology

The roles of AT&T interviewees included:

- Chief Architect
- Director of Cloud Engineering
- Director of Cloud Operations
- Director of Security Operations Center
- Chief Information and Security Officer

A.3.4 Analyses

The analysis phase of the evaluation included: an analysis of the scorecard, a “Blue Team” analysis, analysis of the security architecture using NIST CSF’s profiles, and an analysis leveraging the MITRE ATT&CK Framework®.

A.3.5 Scorecard Analysis

The scorecard is the primary mechanism to assess whether AT&T is meeting its contractual requirements related to cybersecurity. The scorecard is produced twice a year (once as a draft, and the second time as a final deliverable) and scored annually. Two versions of the scorecard were included in the analysis: July 2020 and March 2021. The March 2021 version was a draft (due to be finalized in May 2021, after MITRE’s fieldwork period).

MITRE used the scorecard in three separate analyses:

1. A mapping of the scorecard to the contract's cybersecurity requirements.
2. A comparison of the scorecard content to the NIST CSF as an industry standard in terms of what should comprise and be measured in a good security architecture.
3. An assessment of the requirements scoring in the scorecard.

Mapping of the Scorecard to the Contract

The purpose of mapping the scorecard to the contract was to determine how comprehensive the scorecard is in terms of including the contractual cybersecurity requirements, and whether any requirements are missing from the scorecard. The analysis included a review of the entire contract to identify any security requirements that were outside of the cybersecurity section. The mapping of the scorecard to the contract's specific cybersecurity section involved a line-by-line review of the scorecard and contract to identify any cybersecurity requirements not in the scorecard.

Comparison of the Scorecard to NIST CSF

The CSF provides a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls that the owners and operators of critical infrastructure may adopt to help them identify, assess, and manage cyber risks.[35] The comparison of the scorecard to the NIST CSF involved mapping the CSF sub-categories to specific requirements in the scorecard. MITRE categorized the mappings into three buckets:

- NIST CSF sub-categories that clearly mapped to scorecard requirements
- NIST CSF sub-categories that partially mapped to scorecard requirements
- NIST CSF sub-categories that did not map to scorecard requirements

In MITRE's analysis, the team also looked at the NIST CSF sub-categories that did not map to scorecard requirements (the third bucket above) to determine if they were covered by any of the architecture documents FirstNet Authority provided to MITRE. Additionally, MITRE identified vulnerabilities associated with the NIST CSF sub-categories that did not map to scorecard requirements.

Assessment of the Requirements Scoring in the Scorecard

MITRE analyzed each of the requirement scores and the overall score to determine how well AT&T is performing against the scorecard requirements. MITRE reviewed the scoring overall and at a requirement level; however, MITRE did not review how FirstNet Authority created the rating system or its reasoning for scoring items. Based on FirstNet Authority's stated standard, i.e., a score of 3 or above on a scale of 0 to 4 (4 being the highest and 3 being the standard set by FirstNet Authority), MITRE grouped the requirements that scored a 1 or 2 (note: no requirements scored a 0). MITRE also identified vulnerabilities associated with each low-scoring requirement.

[35] NIST, April 2018.*Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1)*.1

A.3.6 Blue Team Analysis

The analysis identified threats relevant to the NPSBN, principally threats to cellular network infrastructure and services. The Blue Team analyzed these threats against the known state of security controls and practices used to protect NPSBN. MITRE then prioritized the threats most likely to impact NPSBN security.

In identifying threats, MITRE leveraged the scorecard and associated analysis. MITRE also referenced best practices in cybersecurity performance management as published by the SANS Institute, Center for Internet Security (CIS), and NIST. MITRE also reviewed documents FirstNet Authority provided, including the CDSA. In addition, MITRE leveraged external sources, including IEEE, NIST Special Publications, FirstNet.gov, MITRE ATT&CK Framework®, laws, and interview notes.

MITRE used the Mobile ATT&CK Framework® to identify threats to FirstNet Authority devices, while simultaneously applying the ATT&CK Enterprise Framework to identify vulnerabilities within the architecture itself. MITRE categorized the specific threats and vulnerabilities into six buckets:

- General
- Threats to Cellular Infrastructure
- Jamming
- Eavesdropping
- Rouge Base Stations
- Passpoint Wi-Fi

As with all parts of the evaluation, MITRE was only able to review documents FirstNet Authority provided. The evaluation was "paper-based" in that MITRE did not have access to any systems or networks. b(7)(e) [redacted]

A.3.7 CSF "As Is" and "To Be" Profiles

The creation of the CSF "As Is" and "To Be" profiles included a review of the NPSBN security architecture and associated cybersecurity threats and risks, including the following tasks:

- Develop a generic security architecture description derived from best commercial practices and documentation of viable security architecture components from CSF, SANS, and CIS.
- Map architecture components to CSF functions, categories, and sub-categories to demonstrate how CSF can be an effective framework to describe a security architecture.
- Review available contract and technical documentation that FirstNet Authority and AT&T provided and conduct programmatic and technical interviews with FirstNet

Authority and AT&T staff to understand the security capabilities and concepts used to design, implement, and operate the NPSBN.

- Compare CSF categories and sub-categories against the NPSBN security architecture components and capabilities to develop an "As-Is" view, or CSF Profile, of the security architecture.
- Compare the NPSBN "As-Is" profile to the Generic Security Architecture to identify missing or potentially incomplete architecture components.
- Develop a proposed NPSBN "To-Be" profile, including capabilities and features that AT&T and/or FirstNet Authority stated will be part of planned upgrades to NPSBN, as well as suggested components that may be missing or are partially complete.

A related but separate sub-task reviewed how security architecture components can be used with a cybersecurity framework describing the TTPs malicious actors commonly used to probe and exploit information technology (IT) system and software vulnerabilities. These TTPs could be combined with NPSBN vulnerabilities that, if left unmitigated, would result in unacceptable levels of risk for adverse actions such as denial or loss of NPSBN services to first responder subscribers; exfiltration of subscriber personal and operational information could lead to a loss of effectiveness for subscribers and associated public safety activities, and to exfiltration and cyber-espionage of proprietary technical and financial information belonging to both AT&T and FirstNet Authority. This sub-task used the MITRE ATT&CK Framework® as the basis for analyzing these malicious TTPs. Further research could be done in this area but is currently out of scope for this evaluation.

b(7)(e) [redacted]

[redacted]

[redacted]

[redacted]

b(7)(e)

b(7)(e)	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

b(7)(e)	[redacted]	[redacted]
		[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]

b(7)(e)

b(7)(e)	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]

b(7)(e)

b(7)(e)	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]

Appendix B Industry Standards and Frameworks

B.1 Standards

MITRE conducted this evaluation according to its established standards for the conduct of evaluations, which are well-aligned and consistent with the Council of the Inspectors General on Integrity and Efficiency, *Quality Standards for Inspection and Evaluation* (Blue Book) (January 2012, Blue Book). Appendix E describes the alignment of MITRE and Blue Book standards.

MITRE also leveraged industry standards and best practices in the evaluation. These included:

B.1.1 National Institute of Standards and Technology (NIST)

MITRE used the NIST Cyber Security Framework (CSF), also known as the "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1," which:

- Provides guidance on risk management principles and best practices.
- Provides common language to address and manage cybersecurity risk.
- Outlines a structure for organizations to understand and apply cybersecurity risk management.
- Identifies effective standards, guidelines, and practices to manage cybersecurity risk in a cost-effective manner based on business needs.

The Framework, applicable across all organizations regardless of size, industry, or cybersecurity sophistication, can help guide an organization in improving cybersecurity, thereby improving the security and resilience of critical infrastructure.[36]

B.1.2 MITRE ATT&CK Framework®

MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) Framework® "is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations". The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

- MITRE's ATT&CK is a curated knowledge base and model for observed cyber adversary behavior, reflecting the various phases of an adversary's attack lifecycle and the platforms they are known to target. The ATT&CK knowledge base provides an accurate representation of how adversaries conduct operations and empowers defenders to categorize the adversarial actions and relate them to sensors, system configurations, and countermeasures to detect and/or stop those actions.
- ATT&CK was designed around three core precepts—maintaining the adversary's perspective, following real-world adversary behaviors, and bridging offensive action

[36] NIST, April 2018.*Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1)*.v

with defensive countermeasures at the appropriate abstraction level. MITRE collaborates across communities to ensure that the ATT&CK knowledge base remains current and up to date with the latest adversary tactics and techniques.

- ATT&CK is free and open to all organizations to enable it to serve as the foundational understanding of the threat, both internationally and domestically, across a wide range of environments.

The ATT&CK Framework® is a behavior-based threat model and taxonomy of adversary techniques and defensive countermeasures that supports adversary emulation, evaluation of defensive coverage, and other threat-based analytics. ATT&CK informs this analysis with several adversary techniques relevant to cellular networks, apps, and devices, along with information on countermeasures to prevent them and real-world examples of their use. Both the ATT&CK Enterprise and Mobile matrices were used in this analysis.[37]

B.1.3 Center for Internet Security (CIS)

The Center for Internet Security (CIS) publishes commonly accepted security practices. CIS controls are a relatively short list of high-priority, highly effective defensive actions that provide a "must-do, do-first" starting point for every enterprise seeking to improve their cyber defense.[38]

B.1.4 International Organization for Standardization (ISO)

ISO 27001 – ISO/IEC 27001 is widely known, providing requirements for an information security management system (ISMS), although there are more than a dozen standards in the ISO/IEC 27000 family. Using them enables organizations of any kind to manage the security of assets such as financial information, intellectual property, employee details, and information entrusted by third parties.[39]

B.1.5 SANS Institute

Launched in 1989 as a cooperative for information security thought leadership, it is SANS's ongoing mission to empower cybersecurity professionals with the practical skills and knowledge they need to make our world a safer place.[40]

B.1.6 The European Union Agency for Cybersecurity (ENISA)

The European Union Agency for Cybersecurity (ENISA) *Threat Landscape for 5G Networks* includes a comprehensive taxonomy of threats to fifth generation (5G) cellular networks. At the time of this writing, the NPSBN is primarily a Long-Term Evolution (LTE)/fourth

[37] The MITRE Corporation. *MITRE ATT&CK Framework*.www.attack.mitre.org [online]. (accessed July 26, 2021).

[38] Center for Internet Security. CIS Controls Version 7 [online].www.cisecurity.org/blog/cis-controls-version-7-whats-old-whats-new/ (accessed July 26, 2021).

[39] International Organization for Standardization [online].www.iso.org/isoiec-27001-information-security.html (accessed July 26, 2021).

[40] Sans Institute [online]. www.sans.org (accessed July 26, 2021).

generation (4G) network, so many of the individual threats defined in the Threat Landscape are not applicable. However, the ENISA report also includes a general Threat Map, which can be used to characterize threats to both 4G and 5G networks.[41] Future work could be done to examine how 5G will affect the network as it is implemented over the next two years.

B.2 Other Best Practices and Definitions

MITRE leveraged definitions of:

- **Critical Infrastructure** – according to CISA, and Presidential Policy Directive 21, "The Communications Sector is an integral component of the U.S. economy, underlying the operations of all businesses, public safety organizations, and government." Presidential Policy Directive 21, Critical Infrastructure Security and Resilience, identifies the Communications Sector as critical because it provides an "enabling function" across all critical infrastructure sectors. Based on that directive, both the NPSBN and AT&T are part of national critical infrastructure.[42]
- **Public-Private Partnerships (PPPs)** – There is no binding definition of "public-private partnerships" that spans across all agencies, but an interagency working group has defined them as "collaborative working relationships between the U.S. government and non-federal actors in which the goals, structures, and roles and responsibilities of each partner are mutually determined."[43]
    - There is no "bright line" distinction between public-private partnerships and other forms of collaboration between federal agencies and the private sector. Published resources do not attempt to adopt a definitive definition of public-private partnerships. Ultimately, it is up to agencies to determine what relationships qualify as public-private partnerships and under what circumstances they should draw upon resources.[44]

[41] The European Union Agency for Cybersecurity. Threat Landscape for 5G Networks [online]. www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks. (accessed July 26, 2021).

[42] Cyber and Infrastructure Security Agency [online]. www.cisa.gov/communications-sector (accessed July 26, 2021) and White House.gov. Presidential Policy Directive – Critical Infrastructure Security and Resilience [online]. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (accessed July 26, 2021).

[43] Partnerships Interagency Policy Committee, 2013. *Building Partnerships: A Best Practices* Guide 1 n.1.

[44] For examples of relationships that some agencies consider to be PPPs, consult Occupational Safety & Health Admin., U.S. Department of Labor, Partnership: An OSHA Cooperative Program [online]. www.osha.gov/partnerships/ (accessed July 26, 2021).

Appendix C History and Structure

The Middle Class Tax Relief and Job Creation Act of 2012 (the Act) established FirstNet Authority as an independent authority within the National Telecommunications and Information Administration (NTIA) of the U.S. Department of Commerce, with the duty and responsibility to deploy and operate the NPSBN. The Act authorizes FirstNet Authority to enter a public-private arrangement to construct, manage, and operate the NPSBN.

In 2017, FirstNet Authority awarded a 25-year contract to a major U.S.-based wireless carrier to build, operate, and maintain a wireless broadband network for America's first responders. AT&T is currently in the process of implementing the NPSBN throughout U.S. states and territories. FirstNet Authority's contract with AT&T requires security that meets contract requirements.

The NPSBN consists of two primary networks, the core and the radio access network (RAN). The core network provides infrastructure to interconnect the radio network. The RAN allows subscribers to connect their wireless devices to the network throughout the nation.

The Cybersecurity Objective of the contract is below:

The cybersecurity solution implemented by the Contractor in connection with the contract with the First Responder Network Authority (FirstNet Authority) must comply with the following provision from the Middle Class Tax Relief and Job Creation Act of 2012 (The act):

- Ensure the safety, security, and resiliency of the network, including requirements for protecting and monitoring the network to protect against cyberattack.
- Consult with regional, State, tribal, and local jurisdictions regarding the distribution and expenditure of any amounts required to (establish network policies) regarding the adequacy of hardening, security, reliability, and resiliency requirements.
- Develop recommended minimum technical requirements to ensure a nationwide level of interoperability for the nationwide public safety broadband network (NPSBN). (Section J, Attachment J-3, FCC TAB RMTR)
- Third Generation Partnership Project (3GPP) (section 6001); Long Term Evolution (LTE) (Section 6203); and open, non-proprietary, commercially available standards (Section 6206(b)(2)(B)(i)).

b(7)(e) [redacted]

[redacted]

b(7)(e)

b(7)(e)	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

b(7)(e)	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]

b(7)(e)

b(7)(e) vice

b(7)(e)	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	
[redacted]		[redacted]	[redacted]	
[redacted]		[redacted]	[redacted]	
[redacted]		[redacted]	[redacted]	
[redacted]		[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]	

b(7)(e)	[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]			
[redacted]		[redacted]	[redacted]	[redacted]

b(7)(e)	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]		[redacted]	[redacted]	
[redacted]		[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]	
[redacted]		[redacted]	[redacted]	
[redacted]		[redacted]	[redacted]	

[redacted]

Appendix E Alignment of MITRE and Blue Book Standards

MITRE conducted this evaluation work according to its established standards for the conduct of evaluations and in alignment with the Council of the Inspectors General on Integrity and Efficiency, *Quality Standards for Inspection and Evaluation* (January 2012, Blue Book). Table 8 describes the alignment between Blue Book standards and MITRE standards.

Table 8. Alignment of MITRE and Blue Book Standards

Blue Book Competencies	MITRE Independent Assessment (Evaluation) Standard
Competency The staff assigned to perform inspection work should collectively possess adequate professional competency for the tasks required.	MITRE carefully selects staff who have the knowledge, skills, abilities, and expertise necessary for the task, including assessment (evaluation) methodologies; technical domain; and the ability to quickly develop a working familiarity with the organizations, programs, activities, and/or functions identified for assessment.
Independence In all matters relating to inspection work, the inspection organization and each individual inspector should be free both in fact and appearance from personal, external, and organizational impairments to independence.	Working in the public interest requires MITRE to render impartial services that are free of conflict (MITRE Code of Ethics and Conduct). MITRE maintains strict adherence to the principles of independence—personal, external, and organizational—so that observations, findings, conclusions, and recommendations will be impartial and will be viewed as valid and impartial by knowledgeable third parties.
Professional Judgment Due professional judgment should be used in planning and performing inspections and in reporting the results.	MITRE is committed to exercise reasonable care and diligence and to adhere in all matters to the principles of serving in the public interest. MITRE highly esteems its reputation for maintaining the highest degree of integrity, objectivity, and independence in applying professional judgment to all aspects of its work.
Quality Control Each Office of the Inspector General organization that conducts inspections should have appropriate internal quality controls for that work.	MITRE maintains disciplined internal processes and procedures for ensuring the work performed and the products delivered meet an exceptional quality standard.
Planning Inspections are to be adequately planned.	MITRE follows a disciplined and structured methodology for conducting assessments, beginning with comprehensive planning and preparation that meets well-understood expectations and lays the groundwork for a timely, impactful, and relevant assessment result.
Data Collection and Analysis The collection of information and data will be focused on the organization, program, activity, or function being inspected, consistent with the inspection objectives, and will be sufficient to provide a reasonable basis for reaching conclusions.	MITRE defines key focus areas and points of contention; focuses on answering assessment questions. MITRE considers resources, time, and data available; the need for different expertise; and time to integrate findings and recommendations.

Blue Book Competencies	MITRE Independent Assessment (Evaluation) Standard
Evidence Evidence supporting inspection findings, conclusions, and recommendations should be sufficient, competent, and relevant and should lead a reasonable person to sustain the findings, conclusions, and recommendations.	MITRE considers data-supported, evidence-based analysis as one of the hallmarks of its work. MITRE's disciplined quality standards are designed to ensure sufficient evidence is provided such that any reasonably informed person will concur in the findings, conclusions and recommendations provided.
Records Maintenance All relevant documentation generated, obtained, and used in supporting inspection findings, conclusions, and recommendations should be retained for an appropriate period.	MITRE carefully catalogs and maintains all relevant documentation generated during the conduct of the assessment that is used to support inspection findings, conclusions, and recommendations. All data is carefully controlled and stored in accordance with the sponsor's and MITRE's security policies and sponsoring agreements. There shall be no sharing or release of sponsor sensitive information without express permission by the government, need to know, and appropriate clearance.
Timeliness Inspections should strive to deliver significant information to appropriate management officials and other customers in a timely manner.	MITRE scopes the assessment with consideration of the resources, data availability, and time to integrate findings and recommendations, conduct comprehensive internal and sponsor reviews, and deliver an impactful and relevant assessment result.
Fraud, Other Illegal Acts, and Abuse In conducting inspection work, inspectors should be alert to possible fraud, other illegal acts, and abuse and should appropriately follow up on any indicators of such activity and promptly present associated information to their supervisors for review and possible referral to the appropriate investigative office.	MITRE is committed to performing all work activities to the highest achievable standards and will promptly report any findings that may indicate the possibility of fraud or other illegal acts and abuse.
Reporting Inspection reporting shall present factual data accurately, fairly, and objectively and present findings, conclusions, and recommendations in a persuasive manner.	MITRE will assure all reported findings are represented factually and fairly and are verifiable by multiple unbiased sources.
Follow Up Appropriate follow up will be performed to ensure that any inspection recommendations made to Department/Agency officials are adequately considered and appropriately addressed.	MITRE considers follow-up an important phase in the lifecycle of an assessment and recommends the sponsoring agent solicit the services of MITRE or any reputable independent organization to conduct follow-on activities that increase the likelihood of successful implementation of assessment recommendations.
Performance Measurement Mechanisms should be in place to measure the effectiveness of inspection work.	MITRE considers this competency the responsibility of the sponsoring organization and encourages the same.

Blue Book Competencies	MITRE Independent Assessment (Evaluation) Standard
Working Relationship and Communication Each inspection organization should seek to facilitate positive working relationships and effective communication with those entities being inspected and other interested parties.	MITRE considers the establishment of trust and transparency a critically important first step in the conduct of an assessment. Once these are established, positive working relationships and effective communications with the entity being assessed can thrive.

Source: MITRE

Appendix F Abbreviations and Acronyms

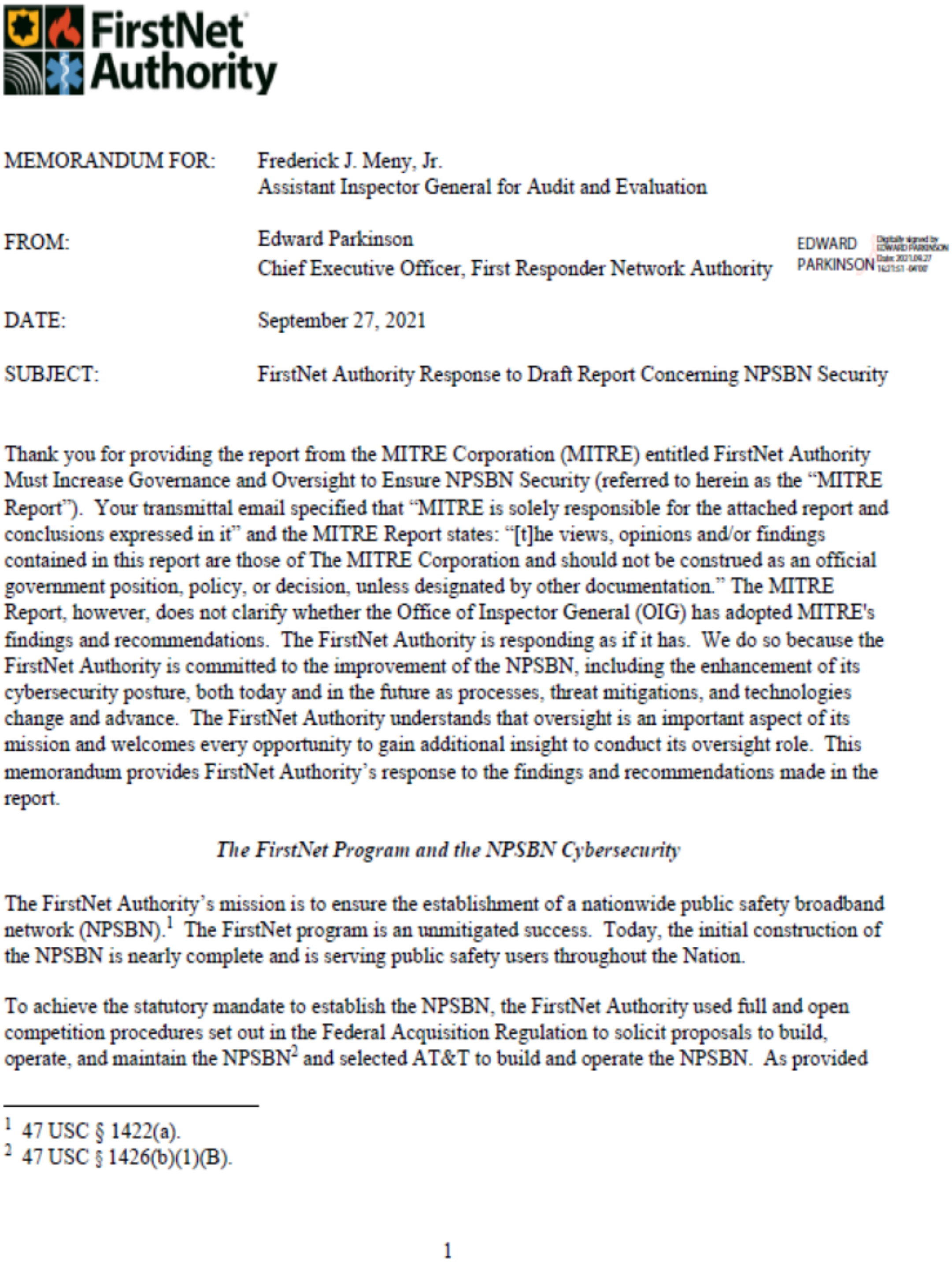
Table 9. Abbreviations and Acronyms

Abbreviation or Acronym	Description
3GPP	Third Generation Partnership Project
AAR	After Action Report
APT	Advanced Persistent Threat
ATT&CK	(MITRE's) Adversarial Tactics, Techniques, and Common Knowledge
BCP	Business Continuity Plan
BMC	Baseboard Management Controller
CDM	Continuous Diagnostics and Mitigation
CDSA	Critical Design Security Annex (also known as Security Reference Guide)
CEO	Chief Executive Officer
CIS	Center for Internet Security
CISA	Cybersecurity and Infrastructure Security Agency
COW	Cell on Wheels
CSF	Cyber Security Framework
CVE	Common Vulnerabilities and Exposures
DDoS	Distributed Denial of Service
The Department	Department of Commerce
DNS	Domain Name System
DoS	Denial of Service
DRP	Disaster Recovery Plan
ENISA	The European Union Agency for Cybersecurity
GAO	Government Accountability Office
ICAM	Identify, Credential, and Access Management
ICMP	Internet Control Message Protocol
IEEE	Institute Electrical and Electronics Engineers
ISCRM	Information Security Continuous Monitoring
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
LTE	Long-Term Evolution
MNO	Mobile Network Operations
OIG	Office of the Inspector General

Abbreviation or Acronym	Description
NIST	National Institute of Standards and Technology
NPSBN	Nationwide Public Safety Broadband Network
NTIA	National Telecommunications and Information Administration
PMR	Program Management Review
PPP	Public Private Partnership
RAT	Remote Access Trojan
RFP	Request for Proposal
RTO	Return to Operations
satCOLT	Satellite Cell on Light Truck
SCRM	Supply Chain Risk Management
SISR	Supplier Information Security Requirements
SLA	Service Level Agreement
SMB	Server Message Block
SMS	Short Message Service
SOC	Security Operations Center
TCP	Transmission Control Protocol
TTP	Tactics, Techniques, and Procedures (reference to ATT&CK)
UDP	User Datagram Protocol

Source: MITRE

Appendix G Agency Response



FirstNet Authority

MEMORANDUM FOR: Frederick J. Meny, Jr.
Assistant Inspector General for Audit and Evaluation

FROM: Edward Parkinson
Chief Executive Officer, First Responder Network Authority

EDWARD PARKINSON Digitally signed by EDWARD PARKINSON Date: 2021.09.27 16:27:51 -04'00'

DATE: September 27, 2021

SUBJECT: FirstNet Authority Response to Draft Report Concerning NPSBN Security

Thank you for providing the report from the MITRE Corporation (MITRE) entitled FirstNet Authority Must Increase Governance and Oversight to Ensure NPSBN Security (referred to herein as the "MITRE Report"). Your transmittal email specified that "MITRE is solely responsible for the attached report and conclusions expressed in it" and the MITRE Report states: "[t]he views, opinions and/or findings contained in this report are those of The MITRE Corporation and should not be construed as an official government position, policy, or decision, unless designated by other documentation." The MITRE Report, however, does not clarify whether the Office of Inspector General (OIG) has adopted MITRE's findings and recommendations. The FirstNet Authority is responding as if it has. We do so because the FirstNet Authority is committed to the improvement of the NPSBN, including the enhancement of its cybersecurity posture, both today and in the future as processes, threat mitigations, and technologies change and advance. The FirstNet Authority understands that oversight is an important aspect of its mission and welcomes every opportunity to gain additional insight to conduct its oversight role. This memorandum provides FirstNet Authority's response to the findings and recommendations made in the report.

The FirstNet Program and the NPSBN Cybersecurity

The FirstNet Authority's mission is to ensure the establishment of a nationwide public safety broadband network (NPSBN).[1] The FirstNet program is an unmitigated success. Today, the initial construction of the NPSBN is nearly complete and is serving public safety users throughout the Nation.

To achieve the statutory mandate to establish the NPSBN, the FirstNet Authority used full and open competition procedures set out in the Federal Acquisition Regulation to solicit proposals to build, operate, and maintain the NPSBN[2] and selected AT&T to build and operate the NPSBN. As provided

[1] 47 USC § 1422(a).
[2] 47 USC § 1426(b)(1)(B).

by the statute, the FirstNet Authority utilized the NPSBN Request for Proposals, AT&T's proposal, and the resulting NPSBN Contract with AT&T to provide for the required solution for the safety, security, and resiliency of the NPSBN network, including protecting and monitoring the NPSBN against cyberattack.[3] As required by statute, the FirstNet Authority also manages and oversees the implementation and execution of the NPSBN Contract with AT&T to build, operate, and maintain the NPSBN.[4]

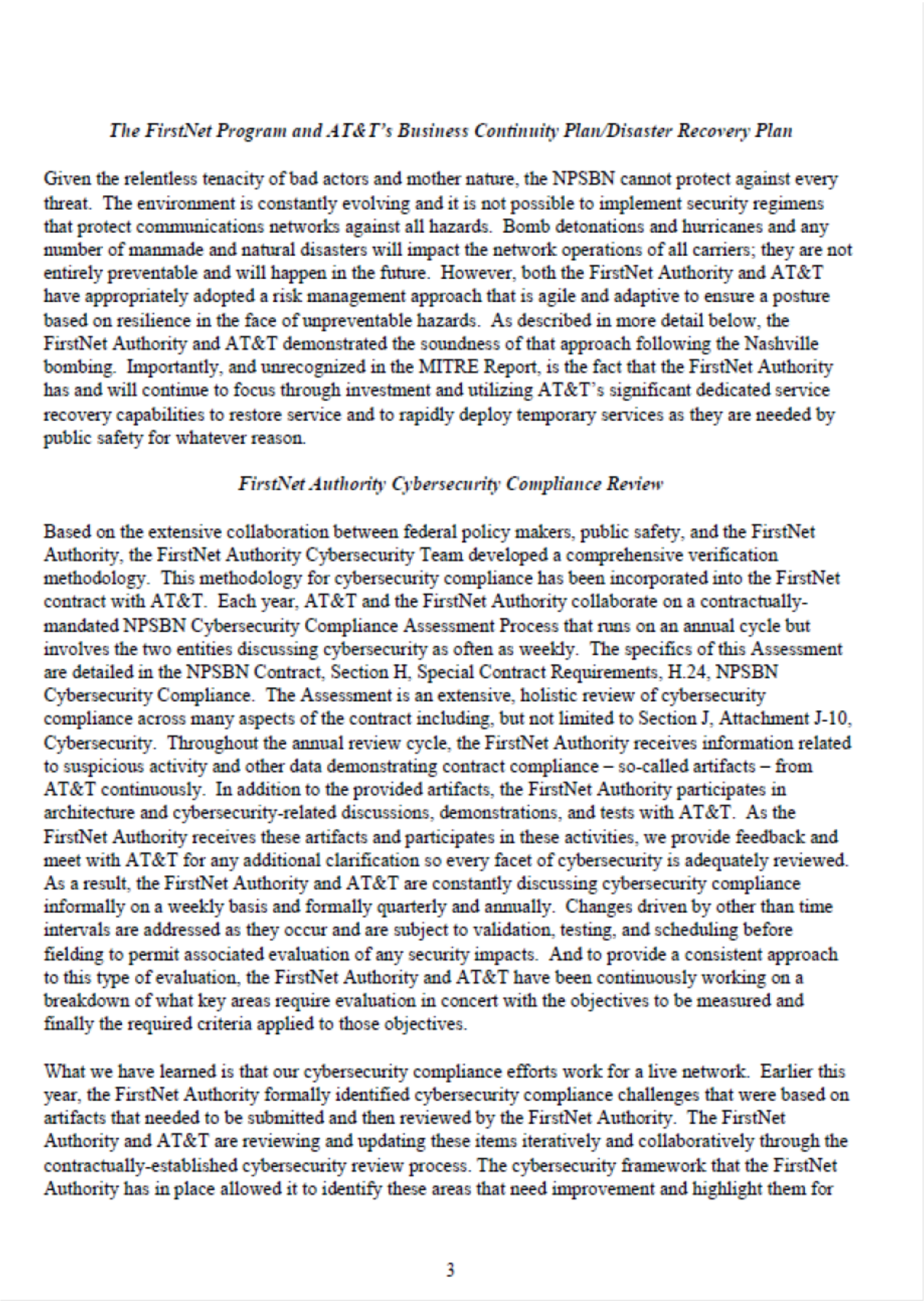
When the FirstNet Authority developed a Statement of Objectives for the NPSBN Request for Proposal, it undertook significant outreach and consultation with subject matter experts and public safety entities. For example, we engaged with the Department of Homeland Security, the Idaho National Labs, the National Institute of Standards and Technology, the Federal Communications Commission, the Public Safety Communications Research Division, and the Department of Commerce. The FirstNet Authority also consulted with a variety of public safety agencies from around the country, as well as the Public Safety Advisory Committee (PSAC).

The result is an NPSBN cybersecurity solution that is designed with a defense-in-depth security strategy, providing protection without sacrificing usability. This is vitally important to the FirstNet program because public safety agencies are often the target of cyber-criminals, hacktivists, and rogue nations. Understanding this, the FirstNet Authority and AT&T have focused on building and operating a highly secure network dedicated to Public Safety. As specified in the NPSBN Contract, AT&T delivers a comprehensive ecosystem solution that takes on much of the network security burden for these public safety agencies. For example, the highly available, redundant, physically separate, dedicated core was designed to comply with many standards-based security regulations and needs, and it will continue to evolve to take advantage of new technologies and address emerging requirements.

In addition, integral to the NPSBN's capabilities is a dedicated Security Operations Center (SOC) as well as a security engineering organization, both staffed by security experts. The SOC monitors and manages NPSBN traffic 24x7x365; employs many of the security systems and procedures that AT&T has honed over decades of operating its highly secure global networks; and focuses primarily on the security needs of the FirstNet program and collaborates closely with engineers working throughout AT&T. More importantly, the NPSBN will be the first-ever large-scale commercial LTE network with comprehensive, tower-to-core encryption based on open industry standards. Commercial networks may encrypt parts of the communications pathway, but only FirstNet will have encryption along the entire route – from the cell tower, through the backhaul, to the core and back again. To achieve this standard, AT&T is rolling out security upgrades on every one of its cell towers across the country with nationwide completion scheduled by the first quarter of 2022.

FirstNet's security requirements are not limited to the network. All applications listed in the FirstNet App Catalog are scanned for malware and security vulnerabilities the first time they are approved for the FirstNet App Catalog. This scan occurs prior to being listed in the FirstNet App Catalog and for every subsequent version of the application, including for minor/bugfix releases. The application is removed from the FirstNet App Catalog if detected discrepancies are not resolved.

[3] 47 USC § 1426(b)(2)(A).
[4] 47 USC § 1426(b)(1)(D).



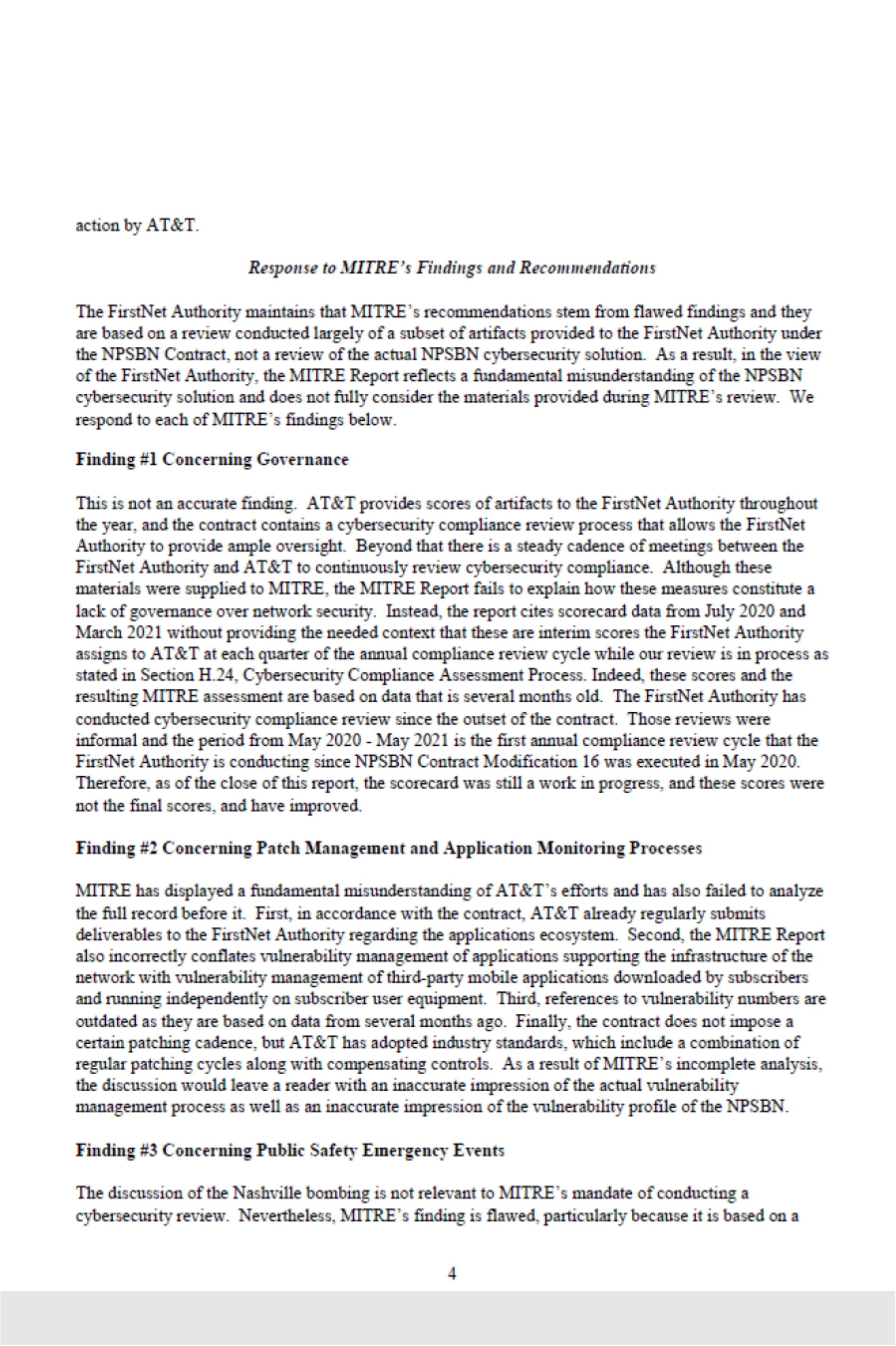
The FirstNet Program and AT&T's Business Continuity Plan/Disaster Recovery Plan

Given the relentless tenacity of bad actors and mother nature, the NPSBN cannot protect against every threat. The environment is constantly evolving and it is not possible to implement security regimens that protect communications networks against all hazards. Bomb detonations and hurricanes and any number of manmade and natural disasters will impact the network operations of all carriers; they are not entirely preventable and will happen in the future. However, both the FirstNet Authority and AT&T have appropriately adopted a risk management approach that is agile and adaptive to ensure a posture based on resilience in the face of unpreventable hazards. As described in more detail below, the FirstNet Authority and AT&T demonstrated the soundness of that approach following the Nashville bombing. Importantly, and unrecognized in the MITRE Report, is the fact that the FirstNet Authority has and will continue to focus through investment and utilizing AT&T's significant dedicated service recovery capabilities to restore service and to rapidly deploy temporary services as they are needed by public safety for whatever reason.

FirstNet Authority Cybersecurity Compliance Review

Based on the extensive collaboration between federal policy makers, public safety, and the FirstNet Authority, the FirstNet Authority Cybersecurity Team developed a comprehensive verification methodology. This methodology for cybersecurity compliance has been incorporated into the FirstNet contract with AT&T. Each year, AT&T and the FirstNet Authority collaborate on a contractually-mandated NPSBN Cybersecurity Compliance Assessment Process that runs on an annual cycle but involves the two entities discussing cybersecurity as often as weekly. The specifics of this Assessment are detailed in the NPSBN Contract, Section H, Special Contract Requirements, H.24, NPSBN Cybersecurity Compliance. The Assessment is an extensive, holistic review of cybersecurity compliance across many aspects of the contract including, but not limited to Section J, Attachment J-10, Cybersecurity. Throughout the annual review cycle, the FirstNet Authority receives information related to suspicious activity and other data demonstrating contract compliance – so-called artifacts – from AT&T continuously. In addition to the provided artifacts, the FirstNet Authority participates in architecture and cybersecurity-related discussions, demonstrations, and tests with AT&T. As the FirstNet Authority receives these artifacts and participates in these activities, we provide feedback and meet with AT&T for any additional clarification so every facet of cybersecurity is adequately reviewed. As a result, the FirstNet Authority and AT&T are constantly discussing cybersecurity compliance informally on a weekly basis and formally quarterly and annually. Changes driven by other than time intervals are addressed as they occur and are subject to validation, testing, and scheduling before fielding to permit associated evaluation of any security impacts. And to provide a consistent approach to this type of evaluation, the FirstNet Authority and AT&T have been continuously working on a breakdown of what key areas require evaluation in concert with the objectives to be measured and finally the required criteria applied to those objectives.

What we have learned is that our cybersecurity compliance efforts work for a live network. Earlier this year, the FirstNet Authority formally identified cybersecurity compliance challenges that were based on artifacts that needed to be submitted and then reviewed by the FirstNet Authority. The FirstNet Authority and AT&T are reviewing and updating these items iteratively and collaboratively through the contractually-established cybersecurity review process. The cybersecurity framework that the FirstNet Authority has in place allowed it to identify these areas that need improvement and highlight them for



action by AT&T.

Response to MITRE's Findings and Recommendations

The FirstNet Authority maintains that MITRE's recommendations stem from flawed findings and they are based on a review conducted largely of a subset of artifacts provided to the FirstNet Authority under the NPSBN Contract, not a review of the actual NPSBN cybersecurity solution. As a result, in the view of the FirstNet Authority, the MITRE Report reflects a fundamental misunderstanding of the NPSBN cybersecurity solution and does not fully consider the materials provided during MITRE's review. We respond to each of MITRE's findings below.

Finding #1 Concerning Governance

This is not an accurate finding. AT&T provides scores of artifacts to the FirstNet Authority throughout the year, and the contract contains a cybersecurity compliance review process that allows the FirstNet Authority to provide ample oversight. Beyond that there is a steady cadence of meetings between the FirstNet Authority and AT&T to continuously review cybersecurity compliance. Although these materials were supplied to MITRE, the MITRE Report fails to explain how these measures constitute a lack of governance over network security. Instead, the report cites scorecard data from July 2020 and March 2021 without providing the needed context that these are interim scores the FirstNet Authority assigns to AT&T at each quarter of the annual compliance review cycle while our review is in process as stated in Section H.24, Cybersecurity Compliance Assessment Process. Indeed, these scores and the resulting MITRE assessment are based on data that is several months old. The FirstNet Authority has conducted cybersecurity compliance review since the outset of the contract. Those reviews were informal and the period from May 2020 - May 2021 is the first annual compliance review cycle that the FirstNet Authority is conducting since NPSBN Contract Modification 16 was executed in May 2020. Therefore, as of the close of this report, the scorecard was still a work in progress, and these scores were not the final scores, and have improved.

Finding #2 Concerning Patch Management and Application Monitoring Processes

MITRE has displayed a fundamental misunderstanding of AT&T's efforts and has also failed to analyze the full record before it. First, in accordance with the contract, AT&T already regularly submits deliverables to the FirstNet Authority regarding the applications ecosystem. Second, the MITRE Report also incorrectly conflates vulnerability management of applications supporting the infrastructure of the network with vulnerability management of third-party mobile applications downloaded by subscribers and running independently on subscriber user equipment. Third, references to vulnerability numbers are outdated as they are based on data from several months ago. Finally, the contract does not impose a certain patching cadence, but AT&T has adopted industry standards, which include a combination of regular patching cycles along with compensating controls. As a result of MITRE's incomplete analysis, the discussion would leave a reader with an inaccurate impression of the actual vulnerability management process as well as an inaccurate impression of the vulnerability profile of the NPSBN.

Finding #3 Concerning Public Safety Emergency Events

The discussion of the Nashville bombing is not relevant to MITRE's mandate of conducting a cybersecurity review. Nevertheless, MITRE's finding is flawed, particularly because it is based on a single event. In fact, AT&T has responded to multiple human and environmental disasters and has recovered any impacted services quickly, efficiently, and with priority. More importantly, as well understood within the Public Safety community, even with best-in-class planning and preparation, unique events occur from time to time that present extreme circumstances that cannot be adequately predicted. The Nashville bombing was one such event, and both the FirstNet Authority and AT&T understand that. These events challenge established and planned response protocols. Despite the damage caused by the Nashville bombing, due to a risk management strategy based on resilience, FirstNet service remained operational immediately following the explosion. The service impact occurred only when the multiple power sources available were all exhausted. Even then, FirstNet deployables enabled service for some locations beginning within four hours. On December 27 and within 48 hours of the service disruption, most communication services were restored including more than 70% of impacted mobility sites. By that same evening, 100% of mobility sites were restored.

When outages occur, the NPSBN is ready because the FirstNet Authority and AT&T place significant attention on disaster recovery. FirstNet's after-action assessment of the recovery from the Nashville bombing found AT&T's recovery response met or exceeded FirstNet's resilience-based risk management standard in the face of an unpreventable hazard. AT&T's response to the bombing began minutes after the blast as personnel responded to initial monitoring alarms, and progressively ramped up during the morning to full disaster recovery protocols and to plan implementation hours before services were disrupted. As part of the disaster recovery capabilities serving public safety that AT&T must provide under the NPSBN Contract, the first mobile transmitting units to arrive on-scene after the Nashville bombing were dedicated FirstNet Satellite Cell on Light Trucks (SatCOLTs). Dedicated FirstNet deployable assets are physically housed across more than 50 strategic sites, optimizing response times nationwide. During the Nashville response, 24 portable cell sites were deployed or staged for support (one within four hours, seven within 24 hours and at the peak, 21 were on-air simultaneously). Additionally, all assets identified for emergent deployment were provided within the 14-hour Recovery Time Objective (RTO) in the NPSBN Contract.

The report also contains inaccuracies which we have previously brought to MITRE's and OIG's attention. If MITRE wishes to identify this event in its report, the report should objectively review AT&T's disaster recovery activities, including the transport (which involves a fleet of trailers and support vehicles) and staging of a Mobile Central Office in Nashville. The disaster recovery capabilities of AT&T are significant. In addition to investment unique and specific to the dedicated FirstNet Deployables program, AT&T has invested more than $650 million in its U.S. Network Disaster Recovery (NDR) program and another $15 million internationally. AT&T Team members have spent more than 145,000 working hours on field exercises and deployments over the last two decades. AT&T is the first company nationwide to receive United States Department of Homeland Security's (DHS) Private Sector Preparedness Program (PS-Prep) certification. Under the circumstances presented, AT&T's response in Nashville was immediate, timely, best-in-class, and contractually compliant. Thus, MITRE's finding is not supported.

Finding #4 Concerning Supply Chain

This finding is fundamentally misdirected, and the hypothetical example lacks any nexus to current or past security threats experienced by AT&T. The current supply chain security posture is based on both federal and global standards in the form of excluding banned vendors of telecommunications components, equipment and software along with ISO 27001 (the international standard on how to manage information security) and ISO 9001 certified supply chain processes (the international standard that specifies requirements for a quality management system). AT&T received ISO 27001 and ISO 9001 certification from an independent auditor. And, under the contract, the FirstNet Authority obtains artifacts from AT&T regarding its supply chain, including AT&T's current ISO 9001 certificate, which was one of the artifacts delivered to MITRE. The FirstNet Authority found AT&T to have the appropriate level of emphasis in protecting the NPSBN from these categories of threats. AT&T has critical measures in place to secure its supply chain, which includes: an initial risk assessment to determine the level of risk associated with a particular supplier as well as mitigation options for any risks identified; mandatory contract language regarding handling of data, setup of hardware and software, and security requirements; and proactive and continuous monitoring of supplier operations that allow AT&T to assess threats and disruptions in real-time.

Given the robustness of AT&T's supply chain practices, the creation of a separate supply chain risk scoring system and associated roadmap, as MITRE recommends, only serve to add overhead with little to no actual added cybersecurity value. Moreover, through the NPSBN Contract, the Government is not purchasing devices or assets from the contractor. Therefore, the FirstNet Authority does not need to develop a digital roadmap to anticipate future supply chain developments. It is AT&T's responsibility to confirm its vendors follow AT&T's comprehensive security policies. It is also AT&T's responsibility to test, implement, and operate devices and software supplied by its vendors.

Conclusion

As explained above, the cybersecurity provisions in the NPSBN Contract have enabled the FirstNet authority to effectively manage and oversee the requirements in Section J, Attachment J-10, Cybersecurity and ensure a compliance regime under Section H, Special Contract Requirements, H.24, NPSBN Cybersecurity Compliance. To further supplement these capabilities, the FirstNet Authority has entered into a contract with a leading cybersecurity firm. This contract was executed to provide the FirstNet Authority with advanced research, technical, and operational expertise concerning cybersecurity-related risks for the NPSBN solution. Our independent 3rd party contractor provides the FirstNet Authority with specialized cybersecurity expertise and provides unbiased advice including essential advanced cybersecurity risk assessment and analysis capabilities to identify, estimate, and prioritize risk related to the infrastructure and operations of the NPSBN. These efforts help supplement the FirstNet Authority's risk identification, assessment, analysis, and mitigation strategies. Our twofold approach the cybersecurity oversight that includes review of artifacts and collaboration with AT&T as well as the receipt of 3rd party expert advice allows the FirstNet Authority to perform its oversight role confidently when conducting cybersecurity-related activities.

The FirstNet Authority will consult with our expert 3rd party cybersecurity contractor concerning the recommendations contained in the MITRE Report. To the extent the report identifies appropriate, actionable, and meaningful issues that would help the FirstNet Authority improve the security of the network, we will evaluate and determine how to implement those in an action plan.

If you have any questions or need additional information, please contact Alice Suh, at alice.suh@firstnet.gov