

THE FRONT LINES OF CONNECTIVITY: EXAMINING FIRSTNET'S ROLE IN PUBLIC SAFETY

HEARING

BEFORE THE

SUBCOMMITTEE ON TELECOMMUNICATIONS
AND MEDIA

OF THE

COMMITTEE ON COMMERCE,
SCIENCE, AND TRANSPORTATION
UNITED STATES SENATE

ONE HUNDRED NINETEENTH CONGRESS

SECOND SESSION

JANUARY 28, 2026

Printed for the use of the Committee on Commerce, Science, and Transportation



Available online: <http://www.govinfo.gov>

U.S. GOVERNMENT PUBLISHING OFFICE

64–226 PDF

WASHINGTON : 2026

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED NINETEENTH CONGRESS

SECOND SESSION

TED CRUZ, Texas, *Chairman*

JOHN THUNE, South Dakota	MARIA CANTWELL, Washington, <i>Ranking</i>
ROGER WICKER, Mississippi	AMY KLOBUCHAR, Minnesota
DEB FISCHER, Nebraska	BRIAN SCHATZ, Hawaii
JERRY MORAN, Kansas	EDWARD MARKEY, Massachusetts
DAN SULLIVAN, Alaska	GARY PETERS, Michigan
MARSHA BLACKBURN, Tennessee	TAMMY BALDWIN, Wisconsin
TODD YOUNG, Indiana	TAMMY DUCKWORTH, Illinois
TED BUDD, North Carolina	JACKY ROSEN, Nevada
ERIC SCHMITT, Missouri	BEN RAY LUJÁN, New Mexico
JOHN CURTIS, Utah	JOHN HICKENLOOPER, Colorado
BERNIE MORENO, Ohio	JOHN FETTERMAN, Pennsylvania
TIM SHEEHY, Montana	ANDY KIM, New Jersey
SHELLEY MOORE CAPITO, West Virginia	LISA BLUNT ROCHESTER, <i>Delaware</i>
CYNTHIA LUMMIS, Wyoming	

BRAD GRANTZ, *Republican Staff Director*

NICOLE CHRISTUS, *Republican Deputy Staff Director*

LILA HARPER HELMS, *Staff Director*

MELISSA PORTER, *Deputy Staff Director*

SUBCOMMITTEE ON TELECOMMUNICATIONS AND MEDIA

DEB FISCHER, Nebraska, <i>Chair</i>	BEN RAY LUJÁN, New Mexico, <i>Ranking</i>
JOHN THUNE, South Dakota	AMY KLOBUCHAR, Minnesota
ROGER WICKER, Mississippi	BRIAN SCHATZ, Hawaii
JERRY MORAN, Kansas	EDWARD MARKEY, Massachusetts
DAN SULLIVAN, Alaska	GARY PETERS, Michigan
MARSHA BLACKBURN, Tennessee	TAMMY BALDWIN, Wisconsin
TODD YOUNG, Indiana	TAMMY DUCKWORTH, Illinois
TED BUDD, North Carolina	JACKY ROSEN, Nevada
ERIC SCHMITT, Missouri	JOHN HICKENLOOPER, Colorado
JOHN CURTIS, Utah	JOHN FETTERMAN, Pennsylvania
BERNIE MORENO, Ohio	ANDY KIM, New Jersey
TIM SHEEHY, Montana	LISA BLUNT ROCHESTER, <i>Delaware</i>
SHELLEY MOORE CAPITO, West Virginia	
CYNTHIA LUMMIS, Wyoming	

CONTENTS

Hearing held on January 28, 2026	Page 1
Statement of Senator Fischer	1
Statement of Senator Luján	2
Prepared statement	3
Statement of Senator Klobuchar	4
Statement of Senator Moreno	29
Statement of Senator Hickenlooper	31
Statement of Senator Budd	33
Statement of Senator Sullivan	42

WITNESSES

Sheriff Michael A. Adkinson, Jr., Acting Chair, First Responder Network Authority Board	5
Prepared statement	6
Scott Agnew, President, FirstNet and Public Safety Mobility, AT&T Inc.	9
Prepared statement	10
Cory Davis, Vice President, Verizon Frontline at Verizon	15
Prepared statement	16
Mel Maier, Chief Executive Officer and Executive Director, APCO International	22
Prepared statement	23

APPENDIX

Letter dated January 21, 2026 to Hon. Ted Cruz and Hon. Maria Cantwell from Jeff Norman, Milwaukee Police Department, President, Major Cities Chiefs Association and Sheriff Chris West, Canadian County, OK, President, National Sheriffs' Association	47
Response to written questions submitted to Michael A. Adkinson, Jr. by:	
Hon. Dan Sullivan	48
Hon. Maria Cantwell	49
Hon. Brian Schatz	49
Hon. John Hickenlooper	52
Response to written questions submitted to Scott Agnew by:	
Hon. Ted Cruz	53
Hon. John Thune	56
Hon. Dan Sullivan	57
Hon. Eric Schmitt	59
Hon. Maria Cantwell	59
Hon. Brian Schatz	61
Hon. John Hickenlooper	65
Response to written questions submitted to Cory Davis by:	
Hon. Ted Cruz	67
Hon. John Thune	70
Hon. Dan Sullivan	70
Hon. Maria Cantwell	71
Hon. John Hickenlooper	71
Response to written questions submitted to Mel Maier by:	
Hon. Maria Cantwell	72
Hon. John Hickenlooper	74
Prepared statement	
, prepared statement	

**THE FRONT LINES OF CONNECTIVITY:
EXAMINING FIRSTNET'S ROLE
IN PUBLIC SAFETY**

WEDNESDAY, JANUARY 28, 2026

U.S. SENATE,
SUBCOMMITTEE ON TELECOMMUNICATIONS AND MEDIA,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Subcommittee met, pursuant to notice, at 10 a.m., in room SR-253, Russell Senate Office Building, Hon. Deb Fischer, Chair of the Subcommittee, presiding.

Present: Senators Fischer [presiding], Sullivan, Budd, Sheehy, Moreno, Luján, Klobuchar, and Hickenlooper.

**OPENING STATEMENT OF HON. DEB FISCHER,
U.S. SENATOR FROM NEBRASKA**

Senator FISCHER. Good morning, I call this hearing to order. Welcome to the Subcommittee, and also to our witness panel today.

I know that Winter Storm Fern delayed this hearing and, I appreciate that you all made it here through a number of obstacles. So thank you very much.

This hearing will examine a critical piece of our national infrastructure, the Public Safety Broadband Network established by the First Responder Network Authority, commonly known as FirstNet. In communities large and small, first responders save lives every single day, often in situations where each second counts and communication means the difference between life and death.

FirstNet was created to give them a dedicated nationwide broadband network that is efficient, reliable, and effective. A network that stands apart from congested commercial systems and prioritizes public safety users first.

Today, with millions of connections operating across all 50 states and U.S. territories, FirstNet has become a communications lifeline for police officers, firefighters, EMS, and other first responders. Its unique features, like priority access during emergencies, are tools that first responders increasingly depend upon. Reauthorizing the network before it sunsets next February means that Congress needs to get to work now. Otherwise, this critical network faces uncertainty, undermining years of investment and trust with public safety.

Beyond simply extending FirstNet's legal authority, we must ask: Are we ensuring the network lives up to its promise? Recent find-

ings by the Commerce Department's Inspector General raise questions about weaknesses in FirstNet's oversight structure.

FirstNet was created as an independent authority within the Commerce Department to balance operational flexibility with accountability. But the Inspector General's findings make clear that the current governing structure has not provided consistent performance oversight.

This is not a critique of the mission, it is a call to improve the function of FirstNet authority. First, we need to understand how we got here. When FirstNet was conceived in the wake of the 9/11 attacks, it was a complex undertaking, a national mission-critical network with strict public safety requirements, uncertain economics, and no proven business model. AT&T was the only mobile carrier willing and able to make a bid that met those needs. The company committed capital, technical expertise, and operational capability to build something that never existed before, without that bid, this network would not exist in its current form.

This is an achievement, but it should not be confused with a blank check. In fact, the scale and importance of the public safety assets that AT&T now operates makes stronger oversight more essential, not less. Reauthorization is not about questioning good faith, it is about ensuring that a network built through public-private partnerships continues to serve its core mission with transparency, resilience, and adaptability.

Finally, we cannot lose sight of the voice of first responders themselves. Independent surveys show overwhelming support from first responders for reauthorizing FirstNet, not because it is perfect, but because the consequences of losing priority network access, well it would be unthinkable.

FirstNet is more than a network, it is part of our national public safety backbone. Reauthorization gives us the chance, not just to maintain continuity, but to improve the network for those who run toward danger so that we can all be safer. Thank you.

I would now like to recognize my friend and Ranking Member, Senator Luján, for his opening remarks. Senator Luján.

**STATEMENT OF HON. BEN RAY LUJÁN,
U.S. SENATOR FROM NEW MEXICO**

Senator LUJÁN. Thank you, Chair Fischer. And also thank you to Chair Cruz, and Ranking Member Cantwell for calling the hearing on this critical issue. And thank you to each of our witnesses who are here today.

Now, the issues that we are talking about today before this committee are critically important, but I cannot go further without acknowledging what is on the minds of people across the country.

One of Alex Pretti's colleagues said, and I quote, "The default look on his face was a smile". Another said: "Alex wanted to be helpful to help humanity, have a career that was a force of good in the world." We all know Alex is dead. He was killed.

Renee Good's mother said that: "Renee was one of the kindest people I have ever known. She was extremely compassionate. She has taken care of people all her life. She was loving, forgiving, and affectionate. She was an amazing human being." Renee is also dead. She was killed.

They are dead because of policy decisions made by President Trump, Secretary Noem, and White House Deputy Chief Stephen Miller.

This administration decided to ignore the pleas of Minnesota's elected leadership and law enforcement by occupying and terrorizing Minnesota. When Federal agents killed these law-abiding Americans, the administration's response was to call Alex Pretti, the VA nurse who held veterans' hands as they died, Trump administration called him quote "A domestic terrorist", and quote, "would be assassin".

What did they say about Renee Good, a poet, a mother of three? They called her a domestic terrorist. There are many lies by people who have no shame, who seem to take pleasure in terrorizing communities, wrecking families, and dividing the American people.

Now, last night, Senator Thom Tillis said what all of us know, that what Secretary Noem has quote, "Done in Minnesota should be disqualifying, it is just amateurish. It is terrible". Senator Tillis is right. And Senator Murkowski, who both said Kristi Noem should resign or she should be fired. I will add one more name to that list, Stephen Miller. Both failed Alex and Renee. Both failed the American people.

Now, I ask my Republican colleagues to join Senators Tillis and Murkowski by speaking up and defending the rule of law and defending our shared humanity. What is happening now is not OK. It is not normal. People can't pretend that. We have a chance to work together to do something here. I don't understand why this is hard. Now is the moment for accountability. We owe that to the families who are grieving their loved ones, and Americans who feel like they don't recognize the country we are living in.

Now, with that, Chair Fischer, and Chair Cruz, and Ranking Member Cantwell, I will stop in this space. And I ask unanimous consent to submit my opening—my prepared opening statement on the topic of today's hearing into the record.

Senator FISCHER. Without objection.

[The prepared statement of Senator Luján follows:]

PREPARED STATEMENT OF HON. BEN RAY LUJÁN, U.S. SENATOR FROM NEW MEXICO

In New Mexico, we are far too familiar with the devastation and destruction that comes with wildfires, flooding and other natural disasters. In those moments, when our first responders run towards danger, when lives are on the line, when seconds matter—communications need to be reliable and resilient. Today's hearing focuses on the reauthorization of FirstNet, our Nation's dedicated public safety network.

Congress created FirstNet in 2012 as a response to the tragedies on 9/11 when firefighters, police officers, and emergency medical personnel were unable to communicate due to incompatible and overwhelmed communications systems. The goal was to build an interoperable nationwide broadband network dedicated to public safety.

As we consider reauthorization, it is essential that we assess whether FirstNet continues to meet its core mission: providing public safety with priority, preemption, and a communications network they can trust in both everyday operations and during disasters.

There is no question that FirstNet has delivered real benefits. But acknowledging FirstNet's importance does not mean suspending oversight. In fact, its importance is exactly why Congress must take a critical look at the facts as we approach reauthorization in February 2027.

My goal today is to hear testimony from our diverse panel of witnesses to help inform Congress on the proper oversight, accountability, and transparency measures that will help structure FirstNet's reauthorization.

We must understand the reliability and resiliency of today's public safety communications. The networks have vastly evolved over the last decades—today we have 5G, satellite connectivity, deployable assets, and software-based solutions that are constantly evolving.

Public safety also relies on these competing communications networks to do their jobs and often subscribe to more than one network to ensure redundancy—because they understand that lack of communication can cost lives.

That's where the other nationwide carriers come in. Verizon's Frontline and T-Mobile's T-Priority are two additional public safety-focused networks that also provide priority and preemption, network slicing, deployable assets, and specialized support for first responders.

This evolution and competition in the marketplace matters. It also underscores why this hearing is so important in addressing whether FirstNet is structured to keep pace with these technological and market changes.

This is why we must also examine the series of findings across multiple reports from the Department of Commerce's Office of Inspector General. These reports raise serious questions about FirstNet's contract oversight and governance.

Oversight is not about undermining FirstNet. It is about strengthening it. We must be thoughtful and willing to listen to the needs of public safety to ensure that we are properly shaping the next generation of public safety communications for years ahead.

Thank you—and again I look forward to hearing from our witnesses.

Senator KLOBUCHAR. Madam Chair.

Senator FISCHER. Senator Klobuchar.

**STATEMENT OF HON. AMY KLOBUCHAR,
U.S. SENATOR FROM MINNESOTA**

I am here because of—I am head of the 9–1–1 Caucus, and I am interested in this hearing. But I did want to thank Senator Luján for his remarks about what is happening in my state. And just say that I have spent a lot of time in the last few weeks with local law enforcement, not just the Minneapolis Police Chief, but our Sheriff's, the Metro Police, and it has become really hard for them to do their normal work. And that is one of the problems with what is happening here.

So I hope that having talked to the White House, that in fact they are going to bring these ICE agents out of Minnesota. They have already started bringing border control out of Minnesota. And then I hope we can work together to overhaul this agency.

And with that, I am going to go to Judiciary and then come back for my questions, Madam Chair. Thank you.

Senator FISCHER. Thank you, Senator Klobuchar, and thank you, Senator Luján, for your comments.

At this time, I would like to introduce our panel of witnesses. Our first witness is Sheriff Michael Adkinson, Acting Chair of the First Responder Network Authority Board. In this role, Sheriff Adkinson leads the FirstNet Authority Board, which oversees the FirstNet network and ensures it meets the needs of the public safety community.

Our second witness is Scott Agnew, President of FirstNet and Public Safety Mobility at AT&T. Mr. Agnew oversees AT&T's management and operation of the FirstNet network, which currently serves more than 7.8 million devices nationwide.

Our third witness is Cory Davis, Vice President of Verizon Frontline. In this capacity, Mr. Davis oversees Verizon's First Responder Communications Services supporting more than 45,000 public safety agencies across the United States.

And our final witness is Mel Maier, Chief Executive Officer and Executive Director of the Association of Public Safety Communications Officials International. He previously served as the vice chair of FirstNet Authority's Public Safety Advisory Committee.

Welcome to all of you. Sheriff Adkinson, you are recognized to give your opening remarks, please.

STATEMENT OF SHERIFF MICHAEL A. ADKINSON, JR., ACTING CHAIR, FIRST RESPONDER NETWORK AUTHORITY BOARD

Mr. ADKINSON. Thank you, Chair Fischer, Ranking Member Luján, Members of the Committee.

As previously stated, my name is Mike Adkinson, and I am the Acting Chair of the FirstNet Authority Board, but in my day job, I am a sheriff, and uniquely a sheriff that oversees professional fire rescue, emergency medical, emergency air medical, as well as 911 communications. What we know is that 25 years ago, as you stated, this Nation suffered an unimaginable tragedy, and out of that tragedy came the opportunity to be better, to take actions that prevent this happening again.

It was the birth of FirstNet. It was the birth of the public broadband safety network. A network built entirely for public safety to ensure that we are able to carry out our mission to protect the men and women of public safety but more importantly to protect the citizens. And that is the ultimate goal of what we are about and what we do.

I can tell you in the decade of its existence almost at this point, I believe it to be a generational success in infrastructure. There are things that I think have made a difference, and I will reference some of those personally in just a moment. But I will say this, at tens of thousands of agencies and millions of users the ability to have interoperable communication is critical, and FirstNet has been a success at that. And I am very proud to be a part of that.

As one of the early opt-in states in Florida, we understood that this was critical. We have seen it at multiple hurricane events, unfortunate tragedies, things that sometimes are unimaginable, the ability for our first responders to communicate is without question a priority, and that is what this network is ultimately about.

You mentioned the Inspector General Report, I would be remiss if I didn't lean into them. I have been on this Board for about a year and a half. There were six new board members that came in, approximately October of last year, and from my standpoint, this is clear that there is one overriding responsibility and that is to maintain the trust integrity of the American people and the efficacy of what we do.

To that end, we instructed the executive director to lean into these reports, resolve these issues. There is no other acceptable answer than, yes. Whatever it takes to resolve these issues, that is what we are going to do. I think we have done a good job of starting working toward that. There is work to be done. Oversight and accountability is critical in any operation, particularly where people's lives are at stake. We do not have the ability to be wrong here. So we have to do what is necessary to improve what we are doing and how we are doing it.

You are not going to hear me say anything other than that. It is unacceptable. And quite frankly, if you are explaining, you are losing, you just need to resolve problems, and that is what we are about.

To that end, as we move toward discussion of reauthorization, I think there are a couple of things that can be considered that I think make practical solutions available to improve the efficacy of what we do. Let me give you an example, I mentioned that there were six new board seats that came on. That is an incredibly difficult way to maintain continuity and consistency when you run a board. We had asked that you consider staggering these terms every 3 years. That was the way the legislation originally intended it. Once it got off cycle the law did not allow, as I understand it, for the Secretary to change it back to 3 years.

Second, we would ask that you consider expanding the role of public safety on this Board. There are three seats, but we would ask that you dedicate five so that the men and women in public safety have a direct and continued priority impact on the reinvestments and where these need to be made. We think that is critical to be successful.

And then last, in regards to a Government standpoint, you know, we use the word “accountability” and we use the words “responsibility”. They are not the same thing. They are entirely different things.

We had asked that—as I said before, there is too many captains on this ship. There needs to be an unambiguous line of authority in the way things are done. I believe this Board, this Authority is capable of making decisions, but we have to have the authority to do that.

And finally, I would leave you with this. As a state that, unfortunately, has suffered hurricanes, and will continue—and they will happen again, we don’t seek perfection, we seek the effort of perfection in everything we do.

And today is the anniversary of the D.C. tragedy, the crash where 67 individuals lost their lives. And I will tell you that FirstNet was there helping monitor those communications, and making a difference, and providing opportunities. That is when the system operates at its best. Thank you.

[The prepared statement of Sheriff Adkinson follows:]

PREPARED STATEMENT OF SHERIFF MICHAEL A. ADKINSON, JR., ACTING BOARD
CHAIR, FIRST RESPONDER NETWORK AUTHORITY

Chairman Fischer, Ranking Member Lujan, and distinguished Members of the Subcommittee, my name is Michael Adkinson, Sheriff of Walton County, Florida and the Acting Board Chair of the First Responder Network Authority. I am honored to appear before you today to provide testimony regarding FirstNet’s role in public safety.

Introduction

Nearly twenty-five years ago, on September 11, 2001, our Nation endured a devastating attack that exposed a critical vulnerability in our public safety infrastructure. America’s first responders answered the call of duty that day, moving toward danger with unwavering courage and selflessness. Yet they were hampered by communication systems that were fragmented, incompatible, and overwhelmed. This failure to communicate cost lives.

In response, Congress made a deliberate and historic decision—guided by the recommendations of the 9/11 Commission and the urgent appeals of the public safety

community—to establish a single, nationwide, interoperable broadband network dedicated exclusively to public safety. That decision became the foundation for legislation creating the Nationwide Public Safety Broadband Network (NPSBN), known as FirstNet.

Today, Congress's vision is an operational reality for our Nation's first responders. FirstNet spans millions of square miles, delivering coverage across urban centers, rural communities, tribal lands, and U.S. territories. The network provides capabilities that public safety did not previously have, including 24/7 priority and preemption for first responders, nationwide interoperability, a dedicated core, on-demand mobile cellular assets, and scalable broadband capacity for mission-critical applications. As of September 30, 2025, over 30,000 public safety agencies and organizations have adopted FirstNet, including where I serve as sheriff in Walton County, Florida.

The Foundation for Success

Congress laid the foundation for FirstNet's success through the Middle Class Tax Relief and Job Creation Act of 2012.¹ The Act created a model that sought to combine private sector innovation with government oversight to ensure performance and coverage standards essential to public safety.

First and foremost, Congress allocated 20 megahertz of nationwide spectrum, now known as Band 14, exclusively for public safety, ensuring first responders have prioritized access to communications when it matters most.

Second, Congress required the FirstNet Authority to be self-sustaining and to collect and reinvest fees generated under its nationwide public safety broadband network contract. The Government Accountability Office estimated that constructing and operating a nationwide public safety broadband network over the first 10 years could cost between \$12 billion to \$47 billion, depending on factors such as business model, use of existing infrastructure, reliability, and coverage.² Congress provided \$7 billion from commercial spectrum auction proceeds for the initial 4G LTE build-out. Additionally, under a public-private arrangement, FirstNet's contractor,

AT&T, agreed to pay approximately \$18 billion over its 25-year contract term for the Band 14 spectrum lease. The FirstNet Authority determines how those funds are reinvested into the network, consistent with the law. This public-private model, initially capitalized with auction proceeds and sustained by contract fees, allows continuous improvements to public safety communications without requiring new taxpayer funding.³

Finally, Congress established a 15-member Board, which I am honored to serve on, composed of leaders from public safety, the private sector, and experts in finance and technology representing state, local, and Federal perspectives. This diverse composition ensures decisions reflect both the operational realities of first responders, and the technical demands of a nationwide public safety broadband network. It is incumbent on the Board to provide strategic direction and rigorous oversight to guarantee (i) that the FirstNet Authority fulfills its statutory mandate and (ii) that the network evolves to meet the changing mission-critical needs of public safety. Through this governance structure, Congress sought to ensure accountability, transparency, and a direct voice for public safety in shaping the future of emergency communications.

FirstNet also demonstrated something critically important that did not exist before its creation: that there *is* a viable market for high-quality, mission-critical broadband services tailored to public safety. By aggregating demand, setting clear performance expectations, and proving that first responders would adopt and pay for a network built to their needs, FirstNet helped catalyze private-sector investment well beyond the confines of the original public safety broadband network contract.

At the same time, success should not breed complacency. We must not rest on our laurels. As technologies evolve and public safety's operational demands grow more complex, there are opportunities to improve how the network is managed, how investments are prioritized, and how performance is measured. Continued vigilance is necessary to ensure that FirstNet delivers a clear net benefit to public safety, that reinvestments are disciplined and aligned with mission needs, and that robust oversight mechanisms remain firmly in place. Congress wisely paired innovation with

¹Pub. L. No. 112-96, Title VI, 126 Stat. 156, see: <https://www.congress.gov/112/plaws/publ96/PLAW-112publ96.pdf>

²GAO Report (2015): Cost estimate range \$12–\$47 billion for construction and operation over 10 years (*GAO-15-407 Highlights PDF*)

³GAO Report (2022): FirstNet statutory requirements and reinvestment responsibilities (*GAO-22-104915*)

accountability in the original statute; honoring that balance means continually asking hard questions, refining governance, and ensuring transparency so that FirstNet remains worthy of the trust placed in it by first responders and the American public.

A Network Built by and for Public Safety

From the start, FirstNet was built with continuous input from the public safety community. The Act requires consultation with federal, state, local, tribal, and territorial stakeholders, and it established the Public Safety Advisory Committee (PSAC) to ensure the network reflects real-world operational needs. Through these channels, public safety informs coverage objectives, network hardening, priority and preemption, mission-critical services, deployable assets, rural and remote coverage, in-building solutions, cybersecurity, and resiliency needed to operate during disasters, major events, and daily incidents. This engagement ensures that FirstNet is not merely a network with public safety features layered on top: it is a purpose-built public safety platform that adapts as threats evolve and technology advances.

The FirstNet Authority also works with public safety officials to plan for major events. Preparations are underway for the 2026 FIFA World Cup soccer tournament in multiple U.S. cities and for America 250 events to ensure mission execution and public safety.

FirstNet Future Investment

The FirstNet Authority has continued to make investments that expand coverage and evolve capabilities. In 2024, the Board approved a multi-year investment initiative to deliver full 5G capabilities via a standalone core, expand mission-critical services, bolster the deployable fleet, enhance in-building coverage, and add new sites to improve reach and reliability. FirstNet also convened coverage enhancement workshops across the country with state and local agencies to drive future investments where public safety needs them most.

Office of Inspector General Oversight

Of course, there remains room for improvement. As members of this Subcommittee well know, the Department of Commerce Office of Inspector General (OIG) has performed significant oversight of the FirstNet Authority since 2014. In 2024 alone, there were four audit reports and two management alerts addressing a range of issues, including contract modifications, coverage objective targets, and device connection targets. These reviews underscore the importance of rigorous oversight of the FirstNet contract.

As the Acting Board Chair, I take these recommendations seriously. My colleagues and I on the Board have directed FirstNet Authority management to resolve and close these recommendations expeditiously and to address the overarching theme identified by the OIG. Our duty to serve the public safety users of FirstNet requires us to provide strong oversight of the network and to not accept excuses, but rather focus on outcomes.

Reauthorization

Under the Act, FirstNet is scheduled to terminate in February 2027, which will create a risk to continued network operations and may result in a potential loss of service for public safety users. Reauthorization presents a prime opportunity to not only affirm Congress's commitment to public safety, but to improve FirstNet and set it up for success for future years. A currency of trust has been developed in the continuity of service provided by FirstNet. It would be hard to overstate the potential risk to public safety if that were to be eroded by a failure of reauthorization. We would risk the collapse of the nationwide interoperability effort the 9/11 Commission sought to address.

The success of FirstNet hinges on private sector innovation paired with rigorous oversight. However, over the past 14 years, there have been persistent challenges with contract oversight and accountability. As Acting Board Chair I have observed that the roles and responsibilities of NTIA, the Board, and the Authority are not well defined in the statute. Bluntly, when everyone is responsible no one is accountable. Reauthorization provides Congress with a clear opportunity to address these challenges directly by clarifying statutory roles, responsibilities, and the chain of command among NTIA, the Board, and the Authority.

Further, the law currently limits reinvestment to the network core or radio access network (RAN). While this made sense in 2012 during the launch of 4G LTE, as we move toward software driven and AI enabled 6G capabilities we risk locking FirstNet into technologies that were state-of-the-art 14 years ago. Expanding reinvestment authorities to include emerging technologies and services, such as cybersecurity enhancements, deployable assets, and advanced analytics will ensure the net-

work continues to meet evolving public safety needs and affords our first responders access to the best possible technology.

There are a host of reforms Congress can consider to codify lessons learned over the past 14 years. This includes a simple but important reform near and dear to my heart—staggering the Board terms across three years to ensure more continuity and consistency among our membership. By way of example, in November of 2024 six new board members were empaneled at the same time. This, as you can imagine, brings serious continuity challenges. I also am a strong believer in the voice that public safety can provide to the Board. While the law requires that three of the board members represent public safety, I encourage Congress to increase this number to five. In practice, this is how the Board is typically staffed and allows the Secretary of Commerce to nominate a broad array of public safety voices to the Board—from police (including local sheriffs like myself and major city police like my fellow board member Chief Norman), to fire, to EMS and 9–1–1. Finally, the administration will be submitting additional views and I will fully support them.

I look forward to discussing these ideas and more today. And, of course, I stand ready to work with Congress and the Members of this Subcommittee to improve the FirstNet program for our first responders across the Nation. Thank you.

Senator FISCHER. Thank you, Sheriff Adkinson.

Mr. Agnew, you are recognized.

**STATEMENT OF SCOTT AGNEW, PRESIDENT, FIRSTNET AND
PUBLIC SAFETY MOBILITY AT AT&T**

Mr. AGNEW. Chairman Fischer, Ranking Member Luján, Chairman Cruz, Ranking Member Cantwell, and Members of the Subcommittee; thank you for the opportunity to appear before you today.

My name is Scott Agnew, and I serve as President of FirstNet and Public Sector Mobility at AT&T. I am responsible for ensuring AT&T fulfills its Federal obligation to deploy, operate, and continuously evolve the FirstNet network for America's first responders.

At the outset, let me be clear, AT&T strongly supports reauthorization of the First Responder Network Authority, and we support so doing well in advance of the February 27th expiration.

Before FirstNet, public safety relied on fragmented radio systems and congested commercial networks that too often fail during disasters. Congress created FirstNet to solve that problem. And today, FirstNet is delivering that vision.

FirstNet represents one of the most successful public-private partnerships in modern infrastructure policy. In 2017, AT&T was selected to build, operate this nationwide public safety network without taxpayer funding. The network was completed on time and on budget in March 2023, and continues to grow and improve. Over the life of the 25-year contract, AT&T expects to invest approximately \$40 billion of its own capital to build and operate FirstNet.

Since 2017, we have built out the network to cover nearly three million square miles, making it hundreds of thousands of square miles on average in commercial networks. This is a critical advantage for rural, tribal, and remote communities. Today, more first responders trust FirstNet to reliably communicate than any other network.

Importantly, FirstNet provides always on priority and preemption across band 14 and all of AT&T's 5G and LT spectrum. So whether it is planned, like major sporting events, or natural disasters like flooding in Texas or Washington State, or wildfires in Montana or New Mexico, first responders can communicate when networks are congested.

In addition, the network will continue to expand. As designed by Congress, the network will evolve based on direct feedback from public safety. The FirstNet Authority has planned to invest more than \$8 billion over the next decade to improve the network. This includes delivery of a physically separated 5G core, our work with AST in Midland, Texas to deliver public safety grade, direct this device satellite connectivity and FirstNet Fusion, the first mission-critical communication platform that will enable unprecedented interoperability across agencies, carriers, and technologies.

The true measure of FirstNet's performance during crisis, during hurricanes Helene and Milton, FirstNet supported more than 260 emergency requests across multiple states, restoring coverage and sustaining public safety communication when commercial networks were strained or unavailable. And during the assassination attempt at the Presidential campaign rally in Butler, Pennsylvania, FirstNet worked as designed. While commercial networks experienced congestions, FirstNet delivered uninterrupted service.

These are not isolated examples. They are result of a network built specifically for and by public safety. AT&T's commitment to public safety is unmatched. We maintained a dedicated FirstNet organization staffed by professionals with public safety and emergency experience. We operate a 24 by 7 security operations center focused on specifically FirstNet traffic, and we provide public safety with a dedicated fleet of deployable assets.

Congress made a bold and necessary decision when it created FirstNet. This vision is now a reality and it is working. For these reasons, we strongly urge Congress to reauthorize the FirstNet Authority, ensure the critical network continues to serve first responders for decades.

Thank you for the opportunity to testify. I look forward to your questions.

[The prepared statement of Mr. Agnew follows:]

PREPARED STATEMENT OF SCOTT AGNEW, AT&T PRESIDENT—FIRSTNET AND PUBLIC SECTOR MOBILITY, AT&T, INC.

Chairman Fischer, Ranking Member Lujan, and Members of the Subcommittee, thank you for the opportunity to appear before you today to provide an update on the FirstNet network and AT&T's essential role in its expansive deployment, strong performance, nationwide coverage, cutting-edge innovations, and lifesaving public-safety impact.

My name is Scott Agnew. I am the President of FirstNet & Public Sector Mobility at AT&T. I lead AT&T's FirstNet organization and am responsible for ensuring that AT&T meets its Federal contract obligations regarding FirstNet's deployment, performance, operations, and public-safety engagement. Today, I will discuss how AT&T is ensuring that FirstNet delivers on Congress's vision to create a resilient, interoperable broadband network for America's first responders and the status of FirstNet's nationwide deployment and adoption. I will also demonstrate that AT&T's commitment to FirstNet extends beyond the contractual requirements and how AT&T has demonstrated its commitment to public safety with its ability to innovate and respond to the ever-evolving public safety needs.

The Public Safety Imperative of FirstNet

Let me begin by stating that AT&T stands with public safety organizations like the International Association of Fire Chiefs (IAFC), National Fraternal Order of Police (FOP), International Association of Chiefs of Police (IACP), International Association of Fire Fighters (IAFF), and many others, and fully supports the reauthor-

ization of the First Responder Network Authority (FirstNet Authority).¹ Due to the critical nature of this network to our first responder community, we support reauthorization in advance of its current 2027 expiration. First responders bravely operate in high-stakes situations (such as terror attacks and natural disasters) where delays in communications can literally mean the difference between life or death to first responders themselves and the people living in impacted communities. Prior to FirstNet, first responders relied on a patchwork of incompatible radio systems and congested commercial networks. In disasters or mass crowd events, commercial networks often become overloaded, leaving public safety agencies struggling to communicate.

Fortunately, Congress established the FirstNet Authority to build a nationwide high-speed broadband network dedicated to public safety—one in which first responders have priority, preemption, dedicated spectrum when they need it, and interoperability. FirstNet is not merely “another wireless network” but a mission-critical infrastructure asset for the Nation’s public safety community.

I could not be prouder of all we’ve accomplished in just 8 years. As discussed in detail below, the FirstNet network has grown from serving zero to nearly 30,600 public safety agencies and direct-support organizations. FirstNet has been on the frontline of countless emergencies and national disasters and has deployed hundreds of portable mobile assets to support our first responders during those events. Importantly, all of this has been accomplished without one dollar of tax-payer funding. While we are proud of our accomplishments to date, we are equally excited about the opportunities ahead, including the 5G network upgrades, the physically separate 5G core, and launch of our new FirstNet Fusion service.

A Successful Public-Private Partnership

January 2026 marks ten years since the FirstNet RFP’s release and the success of the public-private partnership between the FirstNet Authority and AT&T is clear. AT&T stood alone among the four nationwide carriers at the time in answering Public Safety’s call to build a self-sustaining nationwide broadband network, one designed to operate without taxpayer-funding. Together, the FirstNet Authority and AT&T have delivered precisely what the statute envisioned: a network planned with FirstNet Board oversight; the initial build funded through AWS spectrum auction proceeds; executed by AT&T; and maintained on a sustainable footing through AT&T’s Band 14 usage payments. This virtuous cycle continues today. Public Safety informs priorities for the next phase of enhancements; the FirstNet Board approves network upgrades; those upgrades are funded from ongoing sustainability payments; and AT&T executes the approved plans. The result is a resilient, evolving, and fiscally self-sustaining network that demonstrates the enduring strength of this public-private partnership.

FirstNet Deployment, Coverage, and Adoption: Status and Progress

The Initial Build

In March 2023, AT&T completed the initial build of the network both on-time and on-budget. The initial build covered more than 2.91 million square miles across all 50 states, the District of Columbia and the five U.S. territories. Importantly, FirstNet is an all-band solution, meaning public safety has priority, preemption and quality of service on the FirstNet Authority’s licensed Band 14 as well as AT&T commercial 5G and LTE spectrum. This means any commercial investment by AT&T to expand coverage and capacity also benefits first responders on FirstNet.

As part of the initial FirstNet build, AT&T collaborated with small and rural wireless providers to quickly expand the reach of FirstNet and launched 2,000 FirstNet tower sites in rural and tribal areas. In addition, nearly 1,200 new FirstNet towers were deployed in areas state leaders and the public safety community identified as needing additional wireless coverage.

The Next Phase of the Buildout

Since completion of the initial build, the network continues to expand as Congress envisioned. The FirstNet Authority announced the next phase of FirstNet buildout and network evolution that directs \$6 billion over the next ten years for 5G network upgrades; a dedicated, physically separate 5G standalone core; research and development in public safety technology solutions, and over \$2 billion for additional coverage enhancements. To inform the future coverage buildout, the FirstNet Authority has built a First Responder Impact Model to identify potential areas of interest for future tower investment for public safety. The FirstNet Authority is also hosting

¹ <https://www.theiacp.org/sites/default/files/Congressional/IACP%20Urges%20Support%20for%20Preserving%20FirstNet%20in%20Joint%20to%20Congress.pdf>

joint meetings with AT&T and public safety stakeholders in all 50 states, DC, and the five U.S. territories to solicit feedback from public safety and inform the future buildout of FirstNet coverage.

In 2024 as part of the FirstNet Authority's reinvestment announcement, AT&T committed to deploy an additional 1,000 new Band 14 tower sites over 2 years, which were completed ahead of schedule and at no cost to the FirstNet Authority. Today, the FirstNet coverage footprint spans nearly 3 million square miles across urban, suburban, rural, tribal, and territorial areas. The footprint is 200,000 square miles on average larger than competing commercial networks, an area larger than the state of California that is particularly valuable in serving more remote areas. Since the FirstNet buildout began, this effort increased coverage on tribal lands across the United States by more than 64 percent.

The 'ROG' Assets

In addition to our unmatched footprint, AT&T also provides unmatched support to public safety through the AT&T FirstNet Response Operations Group™ also known as the "ROG". The ROG is a dedicated team of former first responders that deploys dedicated network assets at the request of local, state and Federal agencies to ensure connectivity during critical events, whether they are planned events or emergency response events. The ROG assets, which can be requested free of charge by FirstNet subscribed agencies, include:

- A fleet of 190+ deployables that boost FirstNet wireless coverage in the aftermath of an emergency incident or help augment network capacity and coverage during a planned event. This fleet includes SatCOLTs (Satellite Cell on Light Truck), Compact Rapid Deployables (CRDs), mini-CRDs, and other mobile assets, available at no additional cost to subscribing public safety agencies.
- Deployable assets that connect via satellite backhaul and provide FirstNet wireless service; they require minimal setup time and are designed for rapid deployment in disasters or special events.
- And smaller, more portable assets, like the miniCRD unit, for example, that fits in two fortified suitcases that can be easily transported into an emergency area. These assets offer FirstNet LTE coverage up to ½ mile in challenging environments.

The AT&T ROG deployables have been vital in disaster response, special event support, and filling "last-mile" coverage gaps during planned and emergency response events. Below, I will use a few real-world scenarios to illustrate how valuable the deployable fleet is in our response to critical events.

FirstNet in Action

FirstNet adoption continues to grow steadily and currently supports nearly 8 million connections, serving nearly 30,600 public safety agencies and direct-support organizations.

The true measure of FirstNet is not just buildout statistics or its share of eligible users—it is how the network performs during critical events when lives are at stake. Time and again, FirstNet has distinguished itself from commercial offers that are marketed and sold to public safety. FirstNet has proven its value in our Nation's most challenging moments.

Keeping First Responders Connected Through Hurricanes Helene and Milton

In the fall of 2024, two back-to-back storms, Hurricane Helene (Category 4) and Hurricane Milton (Category 3), devastated wide swaths of the Southeast. FirstNet proved it could scale and respond to public safety's needs through network restoration and by deploying Satellite Cells on Light Trucks (SatCOLTs), Compact Rapid Deployables (CRDs), mini-CRDs, and Response Communications Vehicles to restore coverage where towers and power were down. Across Florida, Georgia, the Carolinas, Tennessee, and Virginia, FirstNet supported more than 260 emergency requests from public safety, while FirstNet Strike Teams worked shoulder-to-shoulder with first responders in flooded, storm-ravaged communities. In addition, the state of North Carolina required additional support to restore operations for a Public Safety Answering Point (PSAP) that lost its wireline connection during Hurricane Helene. FirstNet provided reliable connectivity that supported that PSAP's operations for months following Hurricane Helene.

Responding to Catastrophic Flooding in Central Texas

In July 2025, record rainfall caused deadly flooding along the Guadalupe River in South Central Texas. Within hours, the AT&T FirstNet ROG was on the ground,

supporting the Emergency Operations Center in Kerrville, the urban search and rescue (USAR) teams, and deploying SatCOLTs, CRDs, LEO Emergency Communication Portables (LECPs) and an amphibious vehicle to reach isolated areas. More than 20 public safety support requests were answered. In total, more than 20+ portable cell tower assets were deployed. And within 48 hours, AT&T launched a new macro cell tower site in Hunt, Texas to expand area coverage and capacity to support the influx of volunteers, relief organizations, and visitors aiding in the response efforts. Importantly, this site also provides dedicated connectivity for public safety with Band 14—permanently expanding dedicated coverage for first responders in the region. As rescue teams waded into floodwaters, FirstNet delivered the connectivity they needed to coordinate evacuations, communicate across jurisdictions, and keep both responders and residents safe.

Securing Communications During the Assassination Attempt in Butler, Pennsylvania

During the July 2024 assassination attempt at President Trump’s campaign rally in Butler, PA, FirstNet performed exactly as designed. With thousands of attendees overwhelming commercial networks, FirstNet’s always-on priority and preemption ensured uninterrupted communications for hundreds of federal, state, and local first responders. Within minutes of the incident, more than 1,200 instances of First Priority® safeguarded critical calls, protecting first responders from network congestion, and over 11,000 voice and data sessions were completed on FirstNet in just one hour at the peak of the response. Despite network congestion and issues with “calls and texts [being] delayed” on commercial networks, the U.S. House Taskforce on The Attempted Assassination of President Trump found that “law enforcement personnel with FirstNet cellular service did not have notable interference with their connectivity.”² Public safety leaders praised the reliability with which FirstNet enabled reliable communication across agencies—demonstrating why no other network can match its resilience.³

These are just a few of the many instances where FirstNet has delivered for America’s first responders. These real-world scenarios demonstrate how FirstNet enables resilient, mission-critical communications under conditions where commercial networks have struggled.

National Events and Special Security

FirstNet has been used to support communications at large-scale national events—such as presidential inaugurations, Fourth of July celebrations, and major sporting events—where network congestion is a threat on commercial networks due to the voice and data traffic generated by large crowds. In those events, FirstNet’s multi-level priority access and preemption, and the ability to further augment network capacity with deployable assets, ensured public safety agencies had uninterrupted coverage. And with the United States set to host numerous mass events like its 250th anniversary celebration, the 2026 FIFA World Cup, and the 2028 Summer Olympic games, Congress must not fail to reauthorize FirstNet before its expiration in early 2027 as a critical part of that preparation.

Innovation and Evolution

FirstNet has evolved beyond a legacy LTE network into a 5G-enabled architecture with advanced features. Some of the recent innovations and ongoing initiatives include:

- *Enhanced coverage*
FirstNet offers high-power user equipment (HPUE) solutions, for example, FirstNet MegaRange™ and SHIELD MegaFi routers operate on Band 14 and boost connectivity in challenging environments.
- *In-building Solutions:*
As a result of reinvestment by the FirstNet Authority, public safety agencies can receive FirstNet Cell Booster Pros—free of charge—to address in-building challenges and extend the reach of the FirstNet network within police stations, fire departments, and emergency operations centers.⁴

² <https://taskforce.house.gov/sites/evo-subsites/july13taskforce.house.gov/files/evo-media-document/12-5-2024-Final-Report-Redacted.pdf>

³ <https://www.cnn.com/2024/09/26/politics/house-hearing-trump-assassination-attempt#:~:text=In%20the%20minutes%20before%20Crooks,keep%20Trump%20safe%2C%20Moskowitz%20said.>

⁴ To date, more than 12,000 FirstNet Cell Booster Pros have been installed at the request of public safety across America.

- *Network visibility tools*
FirstNet Central includes a Network Status Map, offering subscribers real-time insight into network status, wireless coverage, ongoing maintenance, and the locations of on-air deployables.
- *Satellite direct-to-device testing*
AT&T and its partners (such as AST SpaceMobile) are conducting FirstNet trials of space-based connectivity with the goal to extend coverage directly to first responder devices in extremely remote locations.
- *Local control and dynamic priority allocation*
Incident commanders may dynamically assign priority to responder groups during events. This ensures the most critical teams maintain connectivity when needed.
- *FirstNet Fusion*
AT&T will soon launch FirstNet Fusion, which will enhance public safety communications and takes inter-carrier interoperability to a new level. Fusion combines critical communications capabilities like push-to-talk, dispatch and connected devices into one seamless experience, and will facilitate the ability to unite all first responders across jurisdictions, carriers, and technologies, whether that's during everyday emergencies, large-scale disasters or widely attended events that require cross-agency mutual aid coordination.

These innovations reflect the FirstNet public-private partnership's commitment to continuous improvement, future readiness, and responsiveness to first-responder's feedback and evolving needs.

Economic, Workforce & Community Impact

FirstNet is not just a technical infrastructure; it is a catalyst for broader economic and workforce gains. FirstNet's build-out has leveraged local labor, construction firms, and regional suppliers, driving regional economic activity in rural and urban communities. A 2024 economic impact study estimated that FirstNet deployment has generated nearly 14,000 jobs per year over seven years and produced approximately \$5.6 billion in wages and salaries to date.⁵ The same study estimated \$8.0 billion in net economic output across industries tied to FirstNet's deployment.

These gains are fueled by AT&T's contracting strategy that supports veterans and a variety of business models in deployment, operations, and maintenance. In addition, the network is focused on serving all public safety by ensuring that traditionally underserved communities, like rural and tribal areas, now benefit from the same baseline of reliable communications. FirstNet has lowered barriers to entry for small, rural and resource-constrained agencies to have access to advanced broadband tools and reliable connectivity.

Thus, FirstNet has transitioned from build-out to sustained growth and utilization, with economic benefits beyond the public safety domain.

Oversight and Continuous Improvement

No large-scale infrastructure project is without challenges or opportunities for improvement. AT&T welcomes the rigorous oversight and accountability that the FirstNet program receives. Our performance is regularly evaluated by the FirstNet Authority, which provides ongoing feedback, while the GAO, and the Commerce Department's dedicated OIG conducts ongoing reviews and publicly releases its recommendations, which we take very seriously. FirstNet stands alone in the industry in subjecting itself to such rigorous and public oversight. In addition, we conduct internal assessments and gather valuable input from public safety stakeholders. By receiving feedback from these diverse sources and being held to formal contract requirements, both the oversight and program governance combine to drive continuous enhancements to the program and ensures FirstNet meets the evolving needs of public safety.

Conclusion

Congress' vision of a dedicated nationwide broadband infrastructure for first responders was bold and essential. Today, FirstNet is delivering on that vision. It is a living, evolving network that saves lives, empowers public safety agencies, and strengthens communities at no cost to taxpayers.

⁵ <https://www.forsmarsh.com/wp-content/uploads/2024/03/Economic-Impact-of-FirstNet-RAN-Development-Executive-Summary.pdf> ("FirstNet RAN development was associated with an increase of \$8.0 billion in net economic output across all industries and \$5.6 billion in total wages and salaries for workers and households across the country" (See Table 1); "Building the FirstNet RAN also created an average of 13,877 jobs per year over the 7-year period, with an estimated range of 103 to 28,460 jobs created per year" (See Table 2)).

AT&T is honored to be the steward of this mission. We will continue to listen to public safety needs, expand coverage, drive innovation, and ensure FirstNet remains a trusted, future-proof platform for first responders well into the decades ahead.

We appreciate the Committee's ongoing support and interest, and I look forward to your questions.

Thank you.

Senator FISCHER. Thank you, Mr. Agnew.
Mr. Davis, you are recognized.

**STATEMENT OF CORY DAVIS, VICE PRESIDENT,
VERIZON FRONTLINE**

Mr. DAVIS. Good morning, Chairman Fischer, Ranking Member Luján, and the Members of the Committee. Thank you for the invitation today.

My name is Cory Davis and I am the Vice President of Verizon Frontline. I am here representing more than 45,000 public safety agencies nationwide that trust our network to provide the connectivity that they need to save lives. For over three decades, Verizon has delivered reliable, resilient, and secure public safety communications. This is a partnership earned, not through Federal mandates, but through trust developed alongside those on the front lines. We honor that trust with a network built for resilience and our crisis response team led by former first responders.

Verizon is leading the industry with innovations like nationwide 5G network slicing, our technology creates dedicated capacity reserved exclusively for public safety: enhancing priority, enhancing preemption and quality of service. It ensures first responders have the network access they need during extreme or routine missions. With Verizon Frontline, their mission is our purpose. And as our credo says: We run to a crisis.

In authorizing the FirstNet Authority, we must recognize a fundamental shift since 2012, the old assumption that wireless broadband for public safety required a single government-owned network has evolved. Today, when an agency puts out a contract for bid, they have three or more robust commercial options. This competition has forced us to innovate daily for public safety, driving the development of over 3,000 deployable response assets and enabling enhanced priority and preemption services.

No network, however, is immune to failure, which underscores a critical point. National and homeland security cannot rely on a single point of failure, true resiliency comes from redundancy and allowing first responders to choose communication solutions that meet their needs.

Fostering a vibrant competitive ecosystem with multiple network vendors is crucial so that if one network faces a challenge, first responders can still communicate. My written testimony offers several specific thoughts on reauthorization, but I want to highlight three that are essential for the future of public safety. First, Congress must reinforce resiliency through competition. NTIA should encourage first responders to choose the service that best meets their needs, and over half today choose something other than FirstNet.

Congress must ensure FirstNet Authority does not undercut fair competition by portraying itself as the only solution. More can be

achieved by promoting multi-network ecosystems, not by entrenching a monopoly.

Second, the Authority should be responsive to all public safety, not just the customers of one commercial carrier. The 2012 law mandates that the FirstNet Authority money amounting to tens of billions of dollars has to be channeled back into the network for the sole benefit of FirstNet subscribers.

This made sense when Congress envisioned a single dedicated network. It makes less sense today, where FirstNet rides on top of AT&T's commercial network. If the Authority uses Federal funds to procure physical infrastructure, like towers in a rural area, access to those assets should be available to all public safety providers, and Federal funds should support all first responders regardless of what commercial carrier they choose.

Third, Congress must strengthen oversight and transparency. The FirstNet Authority has faced persistent operational challenges as outlined in the 20 inspector general reports. The reports have identified missed milestones, overpricing, bad investments, network failures, and whistleblower retaliation. Reauthorization is an opportunity to expand NTIA's oversight rule.

We also agree with the National Sheriff's Association and the Major City Chiefs Association that the Authority should be subject to regular congressional review.

In conclusion, let us take stock of what has worked and what has become outdated. Local public safety officials deserve the right to choose the service that best meets their needs and should benefit from the FirstNet program regardless of that choice. First responders collectively benefit from competition in a multi-network ecosystem, giving them the most resilient and reliable communications.

Ask yourselves like we ask ourselves: What is best for public safety professionals that put their lives on the line every day and require the best, most reliable communications possible?

I look forward to your questions.

[The prepared statement of Mr. Davis follows:]

PREPARED STATEMENT OF CORY DAVIS, VICE PRESIDENT, VERIZON FRONTLINE

Good morning Chairman Fischer, Ranking Member Lujan, Chairman Cruz, Ranking Member Cantwell, and the Members of the Committee. My name is Cory Davis and I am the Vice President of Verizon Frontline, Verizon's wireless public safety broadband service. I am responsible for the strategy, operations, and customer experience for the more than 45,000 public safety agencies nationwide that trust our network to provide the mission-critical connectivity they need to save lives. My team has been instrumental in spearheading the deployment of advanced 5G applications and rapid-response connectivity solutions for first responders utilizing Verizon's world-class wireless network. My full bio is attached to this testimony. Thank you for the invitation to appear before the Subcommittee today.

For over 30 years, Verizon has been dedicated to delivering reliable, resilient and secure communications to the public safety community. This is a partnership earned not through Federal mandates, but through decades of service and trust alongside those on the front lines. We honor that trust with a network built for resilience and a crisis response team led by former first responders. Today, we are leading the industry forward with innovations like nationwide 5G network slicing, creating dedicated network capacity reserved exclusively for public safety. This enhances priority, preemption and quality of services, ensuring first responders have the advanced tools they need to operate safely and effectively. With Verizon Frontline, their mission is our purpose. More details on our service:

- Verizon Frontline is available to public safety organizations, first responders, a select group of specialists and other critical organizations. To meet their evolving needs, we work side by side with the public safety community to understand their challenges and build mission-critical connectivity solutions.
- Verizon Frontline customers get the benefit of Verizon's best-in-class mobile network. The investments we make in that network expand the reach and capacity of our Frontline service along with our commercial offerings.
- The Verizon Frontline advanced preemption system gives top priority to first responder connections across 4G LTE and 5G networks. When network demand surges, preemption automatically gives first responder personnel priority access to the network. This helps ensure that public safety can stay on mission, even in times of high network use.
- Verizon Frontline supports network, system, application and device interoperability for public safety across all participating commercial carriers and agencies. Interoperability is crucial to the safety of first responders and the organizations that support them, no matter what network, apps or devices they use. We are continually enhancing our network and capabilities to meet the mission of enabling voice and data interoperability across agencies, jurisdictions, devices and networks.

Separately, Verizon is at the forefront of emergency response technology with our Verizon Frontline Innovation Program. The Verizon Frontline Innovation Program is a first-of-its-kind innovation incubator dedicated to creating 5G-enabled solutions for public safety, as well as connectivity solutions in austere network deprived environments. The program explores new, innovative technologies that provide solutions to public safety agencies. To date, we have worked with over 25 Innovation Partners to evaluate existing products or to ideate on new solutions.

We are committed to serving the public safety community, and are proud to serve the majority of first responders. My testimony will speak to the importance of preserving the benefits of choice, competition and redundancy for our customers and all public safety entities. Verizon believes it is important that local public safety officials have the ability to choose service from us, from AT&T's FirstNet offerings, or from others who best meet their individual needs. Verizon is not here to say that Congress should displace AT&T as the Authority's contract partner or change the terms under which AT&T uses the 700 MHz public safety spectrum for its commercial customers. Rather, our presence at this hearing is driven by our commitment to our First Responders, who need and deserve absolute confidence in their communications networks of choice. Achieving this confidence requires both resiliency, fostered through redundancy, and innovation, driven by competition. Both concepts need to be built into a refresh of the FirstNet Authority and its underlying statute.

I. Evolution of Public Safety Communications

Nearly fifteen years ago, this Committee's work on the Middle Class Tax Relief and Job Creation Act of 2012 helped move public safety communications into the digital age. Before then, public safety relied in large part on dedicated land mobile radio networks for their mission-critical communications. While rugged and largely reliable, those networks were expensive, locked into proprietary standards, and—critically—not interoperable. The public safety communications market also lagged far behind the innovation curve of the commercial sector. As the age of the smartphone and 4G brought new capabilities to commercial mobile wireless customers, first responders remained tied to their shoulder-mounted walkie-talkies.

I witnessed firsthand the post-2012 shift in public safety communications to wireless broadband networks built on common, interoperable standards. This transition to commercial infrastructure, coupled with then-emerging technologies like priority and pre-emption, allowed Verizon and others to bring the power of broadband and smart devices to first responders, solving the interoperability problems that plagued public safety for decades, including on 9/11. And as an added benefit, public safety began to benefit from the massive amounts of capital investment carriers made in their commercial mobile wireless infrastructure. Finally, this shift gave first responders access to the innovation inherent in the smartphone age, powering new emergency response capabilities. For example, Verizon has now brought 5G network slicing to public safety, which offers first responders reliable dedicated capacity, high-priority access to fast communications, a secure connection, and consistent performance when they need it most.

The shift to broadband-based communications built on common Third-Generation Partnership Project (3GPP) standards also facilitated competition among the three major wireless carriers for public safety's business. Today, when a police, fire, EMS, or other public safety department puts up their communications contract for bid,

they have three or more options to choose from. And they have the ability to choose more than one network, to provide another level of redundancy where they seek it. While Verizon is proud that thousands of public safety agencies rely on our network, this competition keeps us on our toes and forces us to innovate daily, like with our new 5G Frontline network slice, our Tactical Humanitarian Operations Response (THOR) rapid response command vehicle, and other cutting-edge communications capabilities.

II. Today's Ecosystem

The public safety offerings in the market today from Verizon, T-Mobile, and AT&T offer similar capabilities. Each carrier leverages its own wireless broadband infrastructure and full portfolio of spectrum assets to provide mobile wireless connectivity to first responders, as well as other customers. The capital expenditure dollars each company invests yearly in network assets and spectrum (over \$200 billion dollars since 2017 in the case of Verizon alone) immediately benefits the first responders who access those networks for their critical communications needs. These investments in new network technologies like 5G, additional capacity, and network expansion and densification enhance not only the ability of Verizon Frontline customers to communicate when disaster strikes, but also our commercial customers on their daily commute.

The services we sell to public safety, though, come with special treatment of their traffic through technologies like prioritizing public safety communications on the network and preempting other traffic when capacity limitations loom. All three carriers rely on international standards like 4G and 5G as the backbone of public safety service, allowing public safety to benefit from the broader digital technology revolution. And Verizon builds its public safety offering in close coordination with our public safety partners who help guide key investment decisions and technical innovations.

It is crucial for the Committee to have a clear understanding of the FirstNet program's current structure. In 2012, the presumption was that effective public safety broadband communications required a government-owned network, and the law that created the FirstNet Authority was designed around that concept. But this concept evolved dramatically when put into practice via the contract that the FirstNet Authority actually signed with AT&T in 2017. Today, there is no stand-alone, government-owned FirstNet network, contrary to what many believe. It's true enough that the Federal government has provided the FirstNet Authority with billions of dollars and 20 megahertz of prime spectrum. And certain network elements may carry FirstNet branding. But AT&T's "FirstNet" service utilizes AT&T's commercial spectrum bands and the network infrastructure is all owned and operated by AT&T. In other words, under the existing contract, neither the government, nor public safety, will own a thing when that contract expires in 2042, despite the billions of dollars in Federal funding invested in the FirstNet program.

This lack of an actual government-owned network raises questions about the ongoing role and responsibilities of the FirstNet Authority. In the years immediately following 2012, the Authority was in startup mode developing the contract for its network partnership and convincing states to join the national FirstNet framework. The statute also meant it to act as steward for the \$7 billion in seed money, and the 20 megahertz of prime 700 MHz low-band spectrum that Congress provided in the statute. The Authority is set to sunset in 2027 absent reauthorization by Congress. As the 2012 Act envisioned, now is indeed the perfect time for this Committee to think about the Authority's mission going forward.

Notably, the FirstNet Authority has faced operational and practical challenges since its inception. Over the last fifteen years, the Office of Inspector General (OIG) at the Department of Commerce has issued 20 reports critical of how the Authority has conducted its work. OIG has documented its concerns about operational questions related to the Authority, including whether it is meeting key network milestones, making justifiable investments into AT&T's network, and, most recently, silencing internal whistleblowers. OIG has also done important work exploring AT&T's network issues and the impact those had on FirstNet by AT&T customers. What OIG has identified are not merely administrative errors but systemic risks that Congress should address because they directly impacted first responder readiness during disasters like the Maui wildfires.

III. The Future of the FirstNet Authority

The national goal of ensuring reliable, secure, interoperable communications for first responders can best be achieved by promoting a multi-network ecosystem rather than moving this competitive marketplace towards a single provider. Built on a solid foundation of competition, multiple networks provide improved reliability and

resiliency that give first responders the confidence that their communications will work when and where needed. Verizon believes that this concept should guide the work of this Committee and Congress as it contemplates reauthorization of the FirstNet Authority.

Every network and platform, no matter how perfectly engineered it is, will have a failure. I know this too well, as Verizon recently experienced a network event that put us far below the standard of excellence our customers expect of us. Similarly, the OIG has documented failures in the FirstNet service, as noted above. We do not highlight these outages to criticize a competitor—we know firsthand that networks are complex and that we all have to strive continually to make them as resilient as possible. We highlight them to prove that *no single network* should be the sole basket for our Nation's safety. Keeping a vibrant, competitive ecosystem with multiple network vendors is crucial to national and homeland security. That competitive ecosystem also fosters rapid innovation, bringing new capabilities to market that keep public safety on the bleeding edge of communications technology.

Verizon strongly encourages the Committee to view reauthorization through the lens of what is best for public safety in the future. What may have been appropriate for the FirstNet Authority during its “startup phase” may no longer make sense today. A reasonable approach to reauthorization includes taking a hard look at the 2012 law and its assumptions to make sure that the law embraces, rather than impedes, the current competitive public safety communications ecosystem. Congress also should review the foundations of the statute, and the work of the Authority, to make sure that it benefits all of public safety, not just AT&T customers.

A. Re-examining the 2012 Act

The structure of the 2012 law is built around the idea that the government would procure a dedicated public safety network in cooperation with a private sector partner. Congress therefore made a number of very specific policy decisions about how the FirstNet Authority would work relative to its belief that there would be a government-owned network as part of the FirstNet program. As just one example, the statute mandates that all funding raised by the Authority through the contract must be channeled back into “the network.”

Under this contract, the Authority's only ongoing source of funds are fee payments from AT&T for exclusive use of the 700 MHz spectrum licensed to the Authority. AT&T uses that spectrum for both its commercial and its public safety customers, and in return is required to pay the Authority fees totaling \$18 billion over the 25-year contract.

The Authority seems to interpret the statute as saying that it can only use its funds (1) for the Authority's operating expenses (estimated to be about \$3 billion or less over the life of the contract) and (2) to support projects conducted by AT&T. Thus, under the status quo, AT&T pays the FirstNet Authority its lease payment, but then the Authority almost immediately returns the vast majority of those payments back to AT&T. In addition, AT&T has received almost all of the \$7 billion that the Act provided to the Authority by Congress in 2012 as seed money, and AT&T also gets to keep the billions of dollars in subscription fees paid by its “FirstNet” customers.

This requirement to reinvest everything back in “the network” is questionable in today's world where the FirstNet service rides on AT&T's commercial network infrastructure. And both OIG reports and leading public safety organizations have raised questions about whether the Authority has been a good steward of these reinvestment funds. OIG, in particular, has questioned the propriety of some of the reinvestment decisions made by the Authority, and concluded that those decisions are not subject to rigorous review and justification. OIG also noted that the Authority has no reason to conduct deep scrutiny of proposals because it is obligated by the law to effectively return the funds to AT&T. Furthermore, OIG said that some of the Authority's investment decisions do not seem to have been guided by a grounded sense of actual public safety needs.

Some, including key public safety organizations, have suggested recently that this reinvestment structure no longer makes sense. They argue that Congress should allow reinvestment dollars to be redirected to broader public safety priorities (even some potentially outside of the FirstNet program). Such a change would not prevent further reinvestment in AT&T's FirstNet service, nor would it mean that its FirstNet subscribers would not benefit from the billions in capital investments that AT&T makes in its network each year. It simply means that Congress should have either the National Telecommunications and Information Administration (NTIA) or the Authority determine how best to use the reinvestment funds so that they benefit all of public safety (including subscribers to AT&T's FirstNet service).

In very stark terms, the first responders today who have chosen other communications services that better meet their needs (which represent a majority of the market) see no direct benefit from Congress's work creating the Authority or from the billions of dollars it is allowed to spend with minimal oversight. To get the benefit of this system, they are forced to abandon their preferred communications solution and migrate to FirstNet. The law should respect the choices of public safety in how to go about saving lives; it should not undercut those decisions or effectively create a single point of failure in public safety communications that impacts national and homeland security. And it makes little sense from a policy perspective for the Federal government, for example, to fund a new tower to close a gap in public safety coverage, but restrict the use of that tower to a single provider. All network providers that serve public safety should have access to that infrastructure.

This Committee has an opportunity to strengthen the FirstNet program by expanding its benefit to the entire public safety ecosystem. By investing in infrastructure that is available to all public safety, the FirstNet Authority can enhance immediate disaster response, rapid communications recovery, or expansion of public safety communications solutions in unserved or underserved areas.

B. Preserving Competition

The pending reauthorization process also offers Congress a chance to reinforce the national priority for resiliency and reliability in public safety communications secured by the robust competition that already exists. Several public safety officials have stressed in comments to this Committee and Congress broadly about how competition among commercial providers has resulted in an overall better public safety communications environment for first responders.

Verizon would propose that the Committee consider taking several actions as part of reauthorization to promote and protect this competitive environment. First, direct NTIA, as part of its public safety mission, to take concrete steps to foster competition and choice among public safety offerings, including eliminating any governmental bias in favor of any specific public safety network provider. For example, NTIA should encourage federal, state, and local agencies to have fully competitive communications service procurements, and the ability to sign up with multiple vendors. Second, NTIA should educate public safety officials about the broad availability of wireless solutions that provide services like priority and pre-emption for critical communications. Finally, Congress should include what would amount to a "technology and carrier neutrality" clause into the reauthorization, prohibiting the use of Federal grant funds to mandate a specific public safety communications provider.

C. Authority Oversight

Additionally, NTIA needs more room to oversee the actions of the FirstNet Authority. Basic NTIA operational oversight of the Authority should be a given. But the 2012 statute created some confusion on this point. That law designated the FirstNet Authority as an "independent entity" housed within NTIA. But the law did not define what it means for the Authority to have this status. Unfortunately, the Authority has frequently operated in a manner that blurs the line between a Federal oversight body and a commercial advocate for its vendor. This misalignment confuses state and local officials and distorts the marketplace.

The Authority asserts that its status as an "independent entity" means it can largely operate free from accountability to NTIA officials, contrary to what NTIA recommends, and even without regard to larger Administration policy objectives. Two major organizations—the National Sheriff's Association (NSA) and the Major City Chiefs Association (MCCA)—expressed their concerns about this lack of transparency and oversight in recent letters to this Committee and the House Energy and Commerce Committee. Clearer oversight responsibilities would also give public safety additional confidence that the legal interpretations and practical actions of the Authority have undergone the appropriate level of scrutiny.

NTIA could use this oversight power to ensure that the Authority is not undermining competition, or positioning AT&T's "FirstNet" offering as the only choice for public safety. As I noted above, every communications network has challenges. If the FirstNet Authority pushes all of public safety directly or indirectly to AT&T's "FirstNet" offering, it up-ends public safety's decision about what meets its needs the best and could result in a single point of failure with dramatic consequences for public safety broadly. A natural disaster, a large-scale cyberattack, or even a local network outage could sever the capabilities of a single network, turning a lifesaving tool into what amounts to a useless piece of hardware. Beyond these critical public safety risks, it is highly unusual for Federal government employees to be engaging

in sales and marketing activities for a single company in an intensely competitive environment.

D. Other Recommendations

As part of the reauthorization process, Verizon suggests that Congress consider a few additional policy recommendations that complement the ones explained above:

- Congress should keep the FirstNet Authority on a regular reauthorization cycle. Reauthorization allows Congress to guide the larger public safety policy path for both NTIA and the FirstNet Authority. We would recommend, given the rapid changes in public safety communications technologies and the market generally, that Congress adopt a reauthorization schedule similar to other government programs. Associated with that, we see no need for Congress to invest additional newly-appropriated taxpayer dollars in, or license more spectrum assets to, the FirstNet Authority.
- Congress should begin thinking about what happens at the end of the FirstNet Authority's contract with AT&T. NTIA and Congress should understand what their options might be when the contract expires, including what assets, if any, would be part of a new contract. The 2012 law sought the help of the Government Accountability Office with respect to the question of whether the FirstNet Authority should be reauthorized; it could do the same with respect to questions about how to plan for the end of the current contract.
- Congress should make sure that Federal officials do not, in the performance of their duties, act in a way that would have the direct or indirect effect of reducing competition in public safety communications. This would go hand in hand with the recommendation above that NTIA ensure that the Authority operates to expand competition, not harm it. And Congress could direct NTIA to educate state and local officials about the importance of keeping fair competition for public safety communications services.

Verizon also supports the recommendations provided to this Committee in a recent letter from NSA and MCCA and attached to this testimony. Those public safety organizations argue that changes are needed to the Authority's mission to ensure that it acts, in the words of the letter, in the best interests of all public safety. They recommend that Congress:

- (1) not give the FirstNet Authority a permanent reauthorization;
- (2) adopt a series of reforms "to ensure that the FirstNet program benefit[s] all public safety, not just the customers of a single commercial carrier" because the current structure of the program has "been exposed as problematic in recent years;"
- (3) prioritize accountability and transparency;
- (4) require a report on the use of capacity of Band 14 (the spectrum band licensed to the FirstNet Authority in the 2012 law);
- (5) require a report on the full range and categorization of FirstNet subscribers;
- (6) "[d]isallow the use of government funds to support contractors, events, and marketing for any carrier"; and,
- (7) repeal grant/procurement requirements that favor the FirstNet partnership.

Given the complexity of the challenges facing first responders, Congress should use the pending reauthorization as an opportunity to promote a reliable and resilient multi-provider ecosystem. Additionally, this reauthorization process is the ideal time for Congress to modify the FirstNet Authority's mission in order to ensure that the FirstNet program benefits all of public safety, not just those choosing to use AT&T's network. This change would enhance our Nation's public safety capacity for all Americans. And additional reforms, like those noted above, can strengthen the overall program and make sure it is operating in the national interest.

Conclusion

The public safety communications ecosystem has matured significantly in the last decade, and much of that change is due to the good work of the Senate Commerce Committee. The pending FirstNet Authority reauthorization process provides the Committee with an opportunity to take stock of what worked and what needs to be updated in light of the rapid technological change that has taken place since 9/11. Importantly, any changes made through reauthorization should be guided by what is best for the police, fire, EMS, National Security, and other public safety professionals that put their lives on the line every day to protect the public, including respecting their decisions about mission-critical communications network partner-

ships. Verizon believes the best approach is to update the FirstNet Authority's mission and the responsibilities of NTIA consistent with the current realities of the public safety communications marketplace; that way Congress can make sure both agencies—and the FirstNet program generally—are working in the best interests of all of public safety.

Thank you for the opportunity to appear before the subcommittee and I look forward to your questions.

Senator FISCHER. Thank you, Mr. Davis.
Mr. Maier, you are recognized.

**STATEMENT OF MEL MAIER, CHIEF EXECUTIVE OFFICER AND
EXECUTIVE DIRECTOR, APCO INTERNATIONAL**

Mr. MAIER. Good morning, Chair Fischer, Ranking Member Luján, Members of the Subcommittee, thank you for this invitation to testify before you today, and I am grateful for this opportunity to talk about APCO International.

APCO International is the world's oldest and largest public safety communications association dedicated to public safety communications starting in 1935 when the technology of the day was AM radio. And when I recall being a Detroit area resident myself of KOP Radio was one of the first broadcast stations out there that gave Detroit Police the opportunity to give—be on the lookouts and calls for service, all while playing music between the calls because they had an entertainment license for AM radio. How we have evolved since then.

We have more than 45,000 members across the United States, in Great Britain, in Canada, across the world. We operate public safety communication systems for law enforcement, fire, EMS, and other public safety associations, and with more than three decades of public service behind me, I have built a career focused on leadership in law enforcement and public safety.

I was appointed the CEO and Executive Director of APCO International in July 2023. Prior to that, I had served as the CTO, managing public safety telecommunications from that technical side. Prior to joining law—or prior to joining APCO, being in law enforcement for 32 years, I was a captain with the Oakland County Michigan Sheriff's Office. I ran the communications, and 911 system, and the P25, that is APCO Project 25 radio system in Oakland County for 6,000 subscribers.

One of the things that I found that during that is that we found that we needed public safety broadband. And when we looked at national public safety broadband many, many years ago, we learned that there was an opportunity. When we looked at this Band 14 option to look at what public safety can do going forward, and FirstNet was created.

I was part of the FirstNet Public Safety Advisory Committee. I had an opportunity to work on the Executive Committee representing law enforcement and helped guide the network's development and implementation for first responders nationwide.

APCO is uniquely qualified to offer an informed perspective on FirstNet's performance. In 2009, we were part of the public safety leadership that urged Congress to establish this dedicated interoperable network. It had to serve the needs of public safety. That is it. That was it. Serve the critical needs of public safety in a manner that could happen nationwide. Very ambitious.

You mentioned that in your opening statement. That is what it was, and it is a success. We are here today to say celebrate that success. We continue to serve a role giving guidance through the Public Safety Advisory Committee as APCO International. Our feedback goes directly to the Board, that goes back into the FirstNet Authority to help build out the services, products that we need in public safety.

APCO urges the swift reauthorization of FirstNet, because quite simply, lives depend on it. Millions, millions of public safety professionals, including APCO members, depend on FirstNet services and equipment in support of their life-saving missions. We use it every day.

I used it in the field when I was a captain with the Oakland County Sheriff. I used it as a commander when I was running the communication center to backhaul Next Generation 911 technologies, over-the-top applications, and to push it from the call taker, to the dispatcher, to the field units. FirstNet works. We always have to be the first in line when congested networks appear. FirstNet has done that.

We continually look to the future and consider how we can make it even stronger. And at the forefront of this is the central question: What would serve public safety? That is the only question we need to ask. And guided by this, we would urge you to continue that reinvestment in the FirstNet network. Continued expansion is essential to ensure that the FirstNet coverage reaches rural, remote, and underserved communities, where it doesn't exist today, it should exist tomorrow, across America.

The smallest of the small emergency communication centers, 911 centers, the police, fire, and EMS, no responder left without this reliable connectivity. Maintaining and improving these network performance and reliability must remain a top priority.

This includes ensuring that consistent coverage, minimizing downtime, and continuing to provide this predictable high-quality service occurs, we encourage that reinvestment in growth. Now, we consider this, that when Congress considers the adoption, performance metrics, and optional benchmarks that address real world public safety needs, do it on the behalf of latency, of coverage, of ensuring that we can get the products and services we need.

I want to thank you for advancing this important conversation about FirstNet reauthorization. I look forward to answering your questions.

[The prepared statement of Mr. Maier follows:]

PREPARED STATEMENT OF MEL MAIER, CHIEF EXECUTIVE OFFICER AND EXECUTIVE
DIRECTOR, APCO INTERNATIONAL

Chair Fischer, Ranking Member Luján, and members of the subcommittee, thank you for the invitation to testify before you today. I am grateful for the opportunity to provide a public safety perspective and represent the Association of Public-Safety Communications Officials, International (APCO). As the world's oldest and largest organization of public safety communications professionals,

APCO represents over 45,000 members who are responsible for building, managing, and operating public safety communications systems for law enforcement, fire, emergency medical and other public safety agencies.

With more than three decades of dedicated public service, I have built a career focused on leadership in law enforcement and public safety communications. I was appointed CEO and Executive Director of APCO in July 2023, serving as APCO's

Chief Technology Officer since 2022. Prior to joining APCO, I served as a law enforcement officer for 32 years and was the captain and chief of public safety communications for the Oakland County Michigan's Sheriff's Office. In addition to my operational leadership, I have played an active role in national public safety initiatives, serving on the FirstNet Public Safety Advisory Committee during its early implementation and later as the Law Enforcement Chair, helping guide the network's development and implementation for first responders nationwide.

APCO is uniquely situated to offer an informed perspective on FirstNet's performance. In 2009, APCO was part of the leadership that joined forces with other major public safety groups to urge Congress to establish a dedicated, interoperable network that could reliably serve the critical demands of public safety. In 2012, Congress passed legislation resulting in FirstNet, the Nation's first and only nationwide broadband network built exclusively for first responders. APCO was an active participant in shaping FirstNet's technical requirements and standards. APCO continues to serve a central role in the FirstNet governance structure through its representation on the Public Safety Advisory Committee, ensuring that the network remains accountable to the public safety users who rely upon it.

APCO urges the swift reauthorization of FirstNet because, quite simply, lives depend on it. Millions of public safety professionals—including many of APCO's members—depend upon FirstNet service and equipment in support of their lifesaving missions. FirstNet supports 7.5 million connections for public safety, covering nearly 3 million square miles, and approximately 30,000 public safety agencies. And FirstNet's users continue to grow year over year. Because FirstNet works. FirstNet provides public safety professionals with priority access to its high-speed broadband network 24 hours a day, 7 days a week, without exception. FirstNet also provides preemption for public safety traffic, ensuring that public safety calls are always first in line when networks are congested.

While FirstNet has been a tremendous success, we must continually look to the future and consider how we can make FirstNet even stronger. At the forefront of this examination is the central question: what would serve public safety?

Guided by this question, APCO urges continued reinvestment in the FirstNet network. Continued expansion of FirstNet is essential to ensure coverage reaches rural, remote, and underserved communities across America. FirstNet should provide network coverage to even the smallest of the small Emergency Communications Centers and law enforcement, fire, and EMS agencies—so that no first responder is left without reliable connectivity. Maintaining and improving network performance and reliability must also remain a top priority. This includes ensuring consistent coverage, minimizing downtime, and continuing to provide predictable, high-quality service during both routine operations and large-scale emergencies. FirstNet must remain resilient, secure, and consistently available so that public safety professionals can rely on it without interruption. APCO also encourages investment in growth and innovation, including the continued expansion of mission critical applications, devices, and connections that enhance situational awareness and operational efficiency. FirstNet has played a key role in bringing innovative technologies to first responders, enabling new tools that improve incident response. Looking ahead, the network must continue to evolve to support advanced communications tools, including 5G and 6G devices, and accommodate increasing data demands. Sustained investment ensures that FirstNet reaches every community across America and that first responders benefit from cutting-edge capabilities that can save lives.

Congress might also consider adoption of performance metrics and operational benchmarks that address real-world public safety needs. These metrics could include network availability and latency during routine day-to-day operations, and network resiliency and performance during disasters and other large-scale emergencies.

Finally, I want to emphasize one aspect of FirstNet that must not change: we must be careful not to chip away at the foundation that has made FirstNet successful—the way in which it is structured. FirstNet's Board of dedicated public safety professionals, guided by the Public Safety Advisory Committee, exemplifies an independent governance model that is responsive, mission-focused, and grounded in the needs of first responders. Regular engagement with public safety users ensures that public safety operational realities inform FirstNet's network management, investment decisions, and performance improvements. This ongoing communication helps FirstNet remain accountable to the public safety professionals who rely on the network every day and ensures that upgrades, expansions, and operational adjustments directly address the needs of first responders in the field.

Thank you for advancing this important conversation about FirstNet reauthorization. Our nation's first responders deserve certainty that they will retain uninter-

rupted access to the dedicated, high-speed broadband communications network they depend upon every day. We therefore urge the swift reauthorization of FirstNet under the continued oversight of the independent FirstNet Authority Board.

Senator FISCHER. Thank you, Mr. Maier.

We will start now with questions from the members of this committee, five minutes.

Competition, where feasible, can be a safeguard for the public and that includes driving innovation and choice for government partners.

Mr. Maier, you have mentioned that FirstNet has already spurred more competition such as for device costs. Do you believe that there are additional areas to introduce competition within the FirstNet system?

Mr. MAIER. I think that what has happened is amazing. We had no one competing for public safety's attention when cellular networks were first formed. I carried a bag phone in my patrol car. That was quite cutting edge. I had 15 minutes a month to use so I couldn't go over. Competition became part of the FirstNet package. When priority and preemption was presented, we had that wireless priority system, the GAT system, all those things that the Federal Government was providing, they are now available through FirstNet.

Senator FISCHER. When you look at the future, though, what do you see as additional devices?

Mr. MAIER. Additional is going to be the continued support for new devices and new technologies being merged into the networks. Competition that can lower costs, competition that can increase the bandwidth in the spectrum that we are using, as well as really coordinating efforts that help predict better outcomes in the field. Communicating against those three networks is terrific. Verizon Frontline, thank you; T-Mobile, T-Priority, that is terrific; FirstNet, that is terrific. Let us get them out in the field in people's hands.

Senator FISCHER. OK. Thank you.

Sheriff Adkinson, if there were more providers within the system, would there be network security tradeoffs if you have more providers in the system? How secure would it be?

Mr. ADKINSON. Yes. Yes. I think there are a couple things to consider when we talk about that. The reality of it is that I don't want a situation like Tyranny of the Commons, right, but when it becomes everybody's responsibility, it becomes no one's responsibility. From an authority standpoint, there has to be very clear lines delineation of who we hold responsible for outcomes. That would be a challenge. Just bluntly, that is a challenge.

Having said that, every option should be reviewed if it is to the benefit of the people we serve. So I don't think that there is anything you would ever say 100 percent no to. But I always am very reticent when we talk about entering into a closed system, leaving the opportunity to point fingers. And I think the responsibility of the Authority is to hold people accountable. And I think that is the sole purpose of it.

I am actually agnostic to the providing of it, quite frankly. That is not my job to decide, pick winners or losers, my job is to make sure, the Board's job is to make sure that we get a delivery of service that meets the needs of the people we serve.

Senator FISCHER. Thank you.

Mr. Agnew, earlier this month, there was news that AT&T decided to work with a new satellite partner to plug the gaps in the FirstNet mobile network. And I am interested in the process that you use to select this partner. Did AT&T seek proposals from other operators to provide this satellite component of the FirstNet system?

Mr. AGNEW. Yes, Senator. We evaluated—

Senator FISCHER. Is that information available to members of this committee?

Mr. AGNEW. No, that is a private RFP with the vendors and we evaluated that solution, and we selected the best solution for public safety that would basically provide the highest level of connectivity, capacity, resiliency, and performance.

Senator FISCHER. So those were your selection criteria there?

Mr. AGNEW. That is correct.

Senator FISCHER. Is the deal exclusive, or will you be considering other providers?

Mr. AGNEW. Currently the deal from a direct to cellular, from a satellite perspective, is with AST. We currently use multiple satellite providers as part of our deployable program. So specific to direct to satellite it will be AST, Senator.

Senator FISCHER. And what is the length of a contract?

Mr. AGNEW. I would have to get back to you on the specific length, Senator.

Senator FISCHER. OK. Thank you. No carrier is immune to outages, Mr. Agnew. We saw Verizon have a major outage across their network. We saw a serious AT&T outage last February, it took down FirstNet. Will you please explain to the Committee how AT&T has implemented changes since that 2024 incident and what that means for FirstNet's reliability as we move forward?

Mr. AGNEW. Absolutely. Thank you for that question, Senator. And after that outage, well, first of all, we prioritize FirstNet over other elements in our network, and the network was up and running for public safety in 2 hours. Subsequent to that significant oversight by the Authority, by the OIG, we are held accountable to the highest standard, the only network held accountable through oversight and after-action reports.

We subsequently communicated exactly what went on, the action plans to address, and we addressed and actually hardened that network. We are obligated by the contract. We are obligated to the oversight to continuously answer that call.

Senator FISCHER. Mr. Davis, do you have anything to add, as representing Verizon?

Mr. DAVIS. Yes, what I would add is—Chairman Fischer is, you know, competition is good for public safety, and in in the state of Nebraska, we have 52 percent market share. So over half of the first responders in New Mexico are—or sorry—in Nebraska are choosing—yes, are choosing Verizon Frontline for their carrier of choice.

And I would say the same around the network outages. This is why we are here. A single-threaded system is a huge concern for national security if we have all of our eggs in one basket.

Senator FISCHER. Thank you. Senator Luján, you are recognized.

Senator LUJÁN. Thank you, Madam Chair.

Mr. Agnew, the contract that AT&T has around FirstNet is with the Federal Government?

Mr. AGNEW. That is correct.

Senator LUJÁN. It is paid for with taxpayer dollars?

Mr. AGNEW. No, it is not. There is no taxpayer appropriated dollars. It is all self-contained and self-funding through the sustainability payments made by AT&T.

Senator LUJÁN. Do you have to make your service available to a government entity to review?

Mr. AGNEW. That is correct. We do. We have to make eligible to government—are you are talking the contract, Senator?

Senator LUJÁN. You just responded to Chair Fischer and saying that some of the information that was asked to share with this committee that it is proprietary. I don't understand how the hell that is possible. You have to share information about how this helps the sheriffs, and police officers, and first responders, whether it is with a satellite company, or if it is with the people you buy coffee from that is for FirstNet, man, and so I just—that is my question, and I will come back to you, you can respond on the record.

So I just hope that we can get to a place, when we are talking about Federal contracts, information is shared here. And like the Chair said, this is an empty check.

Mr. AGNEW. Right.

Senator LUJÁN. We need to make sure that we are delivering the best service to everybody involved.

So my question, Mr. Maier, in your testimony, you state that, “FirstNet must remain resilient, secure, consistently available so that public safety professionals can rely on it without interruption”. And I completely agree with that. Now, the reality is that communication networks have outages. That is something that both the Chair and I have now shared.

We saw recently experience a nationwide outage of Verizon's network in 2024, and a nationwide outage of AT&T's network that also took FirstNet down for several hours. Just a couple points that I referenced. My question to you is, how do the public safety officials prepare for these expected and unexpected outages?

Mr. MAIER. One of the things that we do well is we plan, as a first responder one of my jobs is to make sure that I had more than one way to get things done. More than one tool in the tool box. One of the things that we have seen is that the emergence of land mobile radio, LMR radios, with these push-to-talk solutions over the air of LTE have expanded that capability of our land mobile systems, our LTE systems, and that is a convergence that is still occurring today.

Second we—secondly we look at some of the public safety UHF, VHS systems out there that are really working on these high-band capacity, working with those folks that are really experts at radio. Those are backups to LTE also. We use data systems, we use public safety communication systems that are closed networks sharing logical or diverse paths of physical. But those backups are only backups as they continue to be—need to be used. Those are

redundancies and it should flow seamlessly. We want that to be seamless.

My device, right here, this phone can go between Wi-Fi and the commercial radio system seamlessly. I am talking on a call. I don't even know it. That is what public safety systems are designed to do. And they fall back. They fail over. Building upon that, we need to invest in better resiliency.

The run times of these generators and these batteries at these remote sites, they lose power during a crisis. How long do they run? Those are things we need to know. Can they step up when the surges happen? When we have large volumes of people, we have many first responders on scene, can the capacity then be carried too?

Those are issues that we deal with by preparing for those by having alternate means of communication. We are using services, a software that we are taking down from the cloud, we are using satellite, we have been doing it for 30 years. Those are things that we plan for and we prepare for so when these outages happen, we are ready to communicate.

If it has to go back to turning a light on in the front of the substation so that when you are driving by, you have a call for service, we will do that, too. That is how it used to work. One of the best parts of your question is really about reliability and resiliency and planning, public safety has direct input into the FirstNet network. That is it.

They have direct input through the Public Safety Advisory Committee, the Board, back to FirstNet on how those things are done. We are part of that planning process.

Senator LUJÁN. I appreciate that, Mr. Maier. I have other questions for the other witnesses on preparation for outages. I will submit them into the record, and that will give you time to respond to them as well.

You know, Mr. Maier, you held up your phone there. There is some law enforcement that have an agreement with AT&T. They have an agreement with Verizon. They have an agreement with T-Mobile. And they are rolling with three phones in their cars, and they are just trying to figure out who the hell to call. Maybe that is something that these companies can figure out as well. So that way, if we don't have roaming, when someone picks up the phone, they want someone to answer. They don't have time to keep rolling through all of those devices as well.

Now, all of you testifying here today have acknowledged the multiple reports from the Commerce Department's Office of the Inspector General. The reports have raised serious concerns about FirstNet's Authority's oversight in its contract with AT&T, including failing to independently verify coverage claims, modifying performance metrics, buildout requirements, on, and on, and on.

Mr. Maier, do you believe Congress needs to strengthen FirstNet's oversight framework? And if so, any specific guardrails, and as my time expires here, maybe what I will just do is ask for you to submit that into the records so I can be respectful of my colleagues' time as well. But I have some others I will submit into the record, get to all of you as well. I really appreciate your time being here today.

Mr. MAIER. Thank you. And we do believe that oversight is a feature of the program, it is not a flaw. It is good business.

Senator LUJAN. Appreciate that.

Senator FISCHER. Thank you, Senator Luján. And we may have time later for a follow-up round, too.

Senator Moreno, you are recognized.

**STATEMENT OF HON. BERNIE MORENO,
U.S. SENATOR FROM OHIO**

Senator MORENO. Thank you, Madam Chair.

Mr. Maier, you talked about your phone, and take that question from communications in Ohio, the state spent a lot of resources to build what is called the MARCS Network which is a land mobile radio communication system. That does not have interoperability and seamless transition with FirstNet. Explain how do you see that as a problem?

Mr. MAIER. One of the challenges we have seen with over-the-top applications, and push-to-talk interfaces that they are not based on commonly accepted standards today because they are unique to the manufacturer of the radio, to the manufacturer of the subsystems, but we know that they can be, they can do those workarounds.

The MARC System is terrific at land mobile radio. There is no question. In Oakland County, Michigan we had a P25 Radio, as well as before that had a Harris Radio, we had Motorola and Harris. We were able to use these devices to connect them to push-to-talk solutions over the air, take advantage of LTE. But it was unique, it was expensive, and it is not something everybody can do.

Those are things I would defer to the FirstNet team on how they see that. I know that they have got a product that they are offering. And I have looked at it. I have seen the information on it. It looks like it has a great opportunity to take all of those divergent things and put them into an interoperable cloud to share information, but I would have to defer to them on this, sir.

Senator MORENO. My point asking you first about that was, it is obviously critically important for a first responder, right?

Mr. MAIER. Yes, sir.

Senator MORENO. And so I am obviously jumping to you, Mr. Agnew what—I mean Mr. Adkinson, what is AT&T doing about integrating the MARCS Network into FirstNet—I am sorry, sorry, Mr. Agnew, of AT&T. Sorry about that.

Mr. AGNEW. Senator, thank you for that question. We are very familiar with your network. It is a very strong land mobile network in Ohio. We actually are in the process, as I mentioned in my orals, is launching a product called FirstNet Fusion. This is taking interoperability to the next level.

The foundation of the networks interoperable between commercial networks, the next phase is making it easier, more affordable and scalable for land mobile radio networks. Fusion is going to transform public safety interoperability because it is not going to matter the network. it is not going to matter the carrier. It is not going to matter the technology.

And we are actually working with your state to demonstrate how we are going to make that a reality. We are going to take the interoperability as Mr. Maier was saying and put it in the cloud. That

makes it more affordable, and that makes it easier to manage. When you have disasters come, and you have mutual aid come as you—very well known in the State of Ohio, where you have multiple agencies converging today. They are configuring radios, it could take hours, it could take days to get that communication set up. You need to be able to do it in seconds. And that is the commitment.

Senator MORENO. So what would be the time line for that to happen?

Mr. AGNEW. It is launching in the first half of the year.

Senator MORENO. This year?

Mr. AGNEW. Yes. Yes, sir. And we are actually, like as I mentioned, having discussions with your leadership there, for public safety.

Senator MORENO. Are you confident that by this time next year we should have that fully integrated as the way Mr. Maier described on his phone?

Mr. AGNEW. I am confident the technology be available, and I am confident it will be ready. We will be working with the MARC System because there is some implementations they will need to make on their side, but I am confident in the product.

Senator MORENO. Good. That is good news for Ohio. Taking off of the question from Senator Luján where he asked about taxpayer dollars, and you said it doesn't fund it. Technically, that is not 100 percent accurate. Didn't the Federal Government put \$6.5 billion dollars into this program?

Mr. AGNEW. Yes, thank you for allowing me the chance to clarify. There was auction proceeds, Spectrum auction proceeds that initially funded the program and help with the buildout. Subsequent to that, sustainability payments are made by AT&T in the amount of \$8 billion dollars and that is what is used to fund the Authority and make the necessary public safety investments.

Now, let me be clear on what the investments are. They are specific to FirstNet, specific to the FirstNet elements. They are not for AT&T to run their network. AT&T operates the complete network, our network as well as the FirstNet network as well, which has a complete dedicated core that needs to be operated.

Senator MORENO. Right. And again, I think what Senator Luján was pointing out, not to speak for him, he can speak for himself, is that there was a significant amount of taxpayer money that went into the \$6.5 billion dollars, the monthly subscriptions are with local governments, correct?

Mr. AGNEW. That is correct.

Senator MORENO. So that is taxpayer money. And I think that was the point that was being made. And I just want to give you a chance to clarify that, because this is definitely taxpayer money. And I think when you are spending taxpayer money, there is a different standard for disclosure. I think you have private contracts for anything that you do. But once you are asking the taxpayer to fork over money and pay it to a private company, then there is a responsibility on disclosure. And I just wanted to make certain that we clarify that for the record.

So I appreciate that. And my time is up.

Senator FISCHER. Thank you, Senator Moreno.

Senator Hickenlooper, you are recognized.

**STATEMENT OF HON. JOHN HICKENLOOPER,
U.S. SENATOR FROM COLORADO**

Senator HICKENLOOPER. Thank you, Madam Chair. Thank all of you for being here today, but also for your public service.

Let me start with Mr. Adkinson. As you know well, Boulder, Colorado, is home to many Federal labs that improve our communication service. Institute of Telecommunication Sciences, ITS, Public Safety Communications Research Lab at the National Institute of Science and Technology, campus in Boulder, and then the FirstNet Authority's Lab.

Now, at the FirstNet lab, science and engineers do the R&D and perform a whole variety of tests to ensure the public technologies, of things like drones and mobile towers, are seamlessly integrated across the network. This research, I guess you call it cutting-edge research is possibly possible because of the state-of-the-art facilities, and the equipment, and also and especially do from the highly trained workforce that is there.

So as Board Chair, Mr. Adkinson, how is FirstNet Authority recruiting and retaining the best engineers, and the best scientists at the Boulder Lab to make sure that that our public safety communications network performs as intended?

Mr. ADKINSON. Thank you, Senator. Obviously, you are talking about some of the most technical and capable communication professionals there are, right? And at the end of the day, we reinvest back into our staff because similarly to our vendor, AT&T, we understand that to move to the next level, whether that is Z-axis, whether that is an implication of singularity between LMR, land mobile radio, and these things, it is critical to have the best and brightest.

Now, as far as, you know, how those folks are retained and hired, I have to defer that to NTIA. That is more in their area of operation. But I have to tell you there is quite a bit of discussion among the Board, and I will segregate that, among the Board to say are we being competitive in hiring the best and brightest in what we do, because that is what it takes to drive this forward. And from a taxpayer standpoint, to Senator Moreno's point a minute ago, these are still public funds *i.e.*, it is the public's trust, right, these fees are the public's trust.

And so the Board takes that very seriously that part of this technology at that lab is to make sure that we are getting the best technology from our vendor as well too. So I think it is an opportunity to maintain the best and brightest. That may be something from a salary standpoint, recruitment standpoint, and I may have to go back to NTIA on that, but I absolutely concur that that is what we need.

Senator HICKENLOOPER. And as the network modernizes its towers and network core to improve service to first responders, what role do you see for FirstNet's Lab, you know, what is that role going to play as this modernization goes forward?

Mr. AGNEW. You know, I mean it—this Moore's Law is roughly you know, what, 18 months on obsolescence, the way things are changing now I think the lab is going to be at the cutting edge of

determining what is capable and what are we envisioning. Because I can tell you even six and seven years ago AI was not part of this discussion, it will be part of the discussion going forward.

Senator HICKENLOOPER. OK.

Mr. AGNEW. Both from a national security standpoint as well as the service we provide to our members there. We haven't talked about it, but there is the Internet of Things, and sometimes when we are talking about all these different lines of service, I think people forget that it also includes video cameras, things like body cameras.

I saw a board member who is also a doctor as well, able to perform, you know, medical assistance from 800 miles away.

Senator HICKENLOOPER. Yes, it is amazing.

Mr. AGNEW. That is what is coming.

Senator HICKENLOOPER. Absolutely. Let me switch over to Mr. Agnew, Mr. Davis. So whether someone is hiking in the—you know, the mountain ranges above Telluride, or they are watching a hockey, or a basketball game in the Ball Arena in Downtown Denver, Colorado's first responders are almost always on the frontlines of keeping our citizens safe.

So in public safety emergencies, reliable wireless communications can mean the difference between lives saved or a tragedy striking a community. And that is why transparency, I think, in how communication networks are managed and upgraded is so essential. So Mr. Agnew, Mr. Davis, in delivering communication service to public safety leaders, how would you describe your process for demonstrating where your network coverage is densified and where it really needs upgrades, specific geolocated upgrades?

Mr. AGNEW. Senator, thank you for that question. And FirstNet has unprecedented transparency as we provided—and thank you, Governor, at the time for opting in, we provided state plan portals to demonstrate the exact build over the course of the initial 6 years. We have also provided what is called a network status tool that public safety can look real time for existing coverages.

In addition, through outreach by the FirstNet Authority and AT&T network coverage workshops, we show the public safety community, in Colorado it happened on September 25, where the coverage has been built and where the coverage is going, also during that time, public safety gets to identify the areas that, where they build what we call public-safety-specific sites.

These aren't sites that are economically viable for AT&T, these are where public safety needs it. And so as part of the \$8 billion reinvestment that FirstNet is making over the next 10 years, that is where the sites are going to come from. That is why FirstNet has three—nearly three million miles were covered and 200,000 more.

And in fact, just in the opt-in process alone, just commenting on Colorado, you had 31 specific sites that were built based off of direct feedback from public safety, not corporate, AT&T.

Senator HICKENLOOPER. Good to hear that.

Mr. DAVIS. That is a great question, Senator. And I have spent a lot of time in those mountains of Telluride, so I know very well those challenges.

Senator HICKENLOOPER. Lucky man.

Mr. DAVIS. Yes. So some of the things that we do is we have a process around transparency and capturing customer feedback. We do quarterly roundtables with public safety professionals. So in your great state we have nearly 50 percent of the market share. So over 50 percent—or nearly 50 percent of those first responders are choosing something other than FirstNet. So it is important to hear that feedback on what is working and what is not working.

We also have a wireless network performance tool that shows coverage where you can request physical assets if you need deployable assets. We also work very closely with all the states on the coverage. And this is why it is so important that competition and innovation is important because if FirstNet Authority funds a tower let us say in rural San Juan County, all public safety providers should be able to take advantage of that tower, not just one commercial carrier.

Senator HICKENLOOPER. Fair enough. Thank you.

I yield back the floor.

Senator FISCHER. Thank you, Senator Hickenlooper.

Senator Budd, you are recognized.

**STATEMENT OF HON. TED BUDD,
U.S. SENATOR FROM NORTH CAROLINA**

Senator BUDD. Thank you, Chair. Thanks for holding this hearing. Thank you all for coming up and being part of this panel. Very helpful.

I remember about 15 months ago, Hurricane Helene in Western North Carolina, there is some at the table here, and some in the audience that I reached out to in those early days. Thank you all for your responsiveness. I know there is lessons learned and we will ask about that in a moment.

We do remember how significantly disrupted connectivity was including infrastructure and strained networks, 911 call centers. But I was impressed with the efforts of everybody involved, including FirstNet, Verizon, other carriers, especially our first responders.

So Sheriff, thank you for being here. Thanks for those in uniform today for what you do, not just with improving first responder communications, but what your roles in law enforcement as well.

So Sheriff, your testimony spoke to how FirstNet's 50-Member Board and the Public Safety Advisory Committee has kept first responders, like yourself, deeply involved in the investment and buildout decisions for FirstNet and FirstNet's Fusion seemed like a good example of prioritizing technological upgrades to keep pace with commercial innovation.

So are there areas FirstNet reauthorizations needs to look at to continue to enhance efforts to make sure a nationwide first responder network is keeping pace and giving responders the best tools they need to be successful?

Mr. ADKINSON. Thank you, Senator. I think a couple of things are pertinent in this discussion, which is, again the rate of technology, the way things are changing, products like Fusion give us the opportunity to get what was the ultimate goal here, which is interoperability on demand, right. And I made a joke earlier today, and I will stand by it, which, sometimes words have multiple meanings.

My children love The Princess Bride, right, and sometimes people say interoperability, and I say don't think that word means what you think it means, and the problem is we can ask multiple people and get different answers, right, but from a first responder standpoint a product like Fusion, once it is built out, and the future of things like that, can result in instantaneous connection between multiple modalities.

That is the goal. And so when you are asking what we should be investing in, as well as extending coverage, making it better, deeper coverage, products that allow that instantaneous change, this leveraging of technology, is the things that I think that the FirstNet Authority—Board should be pushing toward. And I don't think you are going to hear anybody argue against that. I mean, I think that is the driving future.

Senator BUDD. Thank you for that.

Mr. Agnew, your testimony talked about lessons learned during Hurricane Helene and also Hurricane Milton. Could you say what some of those lessons were? I know you have shared earlier, but if there is anything else you would like to add as far as lessons learned, and how do those lessons inform AT&T's work with the FirstNet Authority in determining network investments?

Mr. ADKINSON. Yes, Senator, thank you for that question. Lessons Learned, it was a massive event, multiple states, over 260 requests, and as we do a hotwash is what public safety does after an event. And there were almost 89 requests that came in within the first 24 hours. And so that was a lot to triage. So we have determined that we needed multiple triage teams to speed those up. So we have subsequently changed that.

Additionally, we realized we needed more smaller assets to be able to manage that type of event to be able to respond quickly. So we have made the subsequent investment.

The other area we saw is that public safety supported the event. They have their own deployables that they purchase. Your state, Tennessee, Federal agencies came to the table for mutual aid. So we needed to put out and we have subsequently done that more affordable solutions so public safety can put their own coverage out there as well.

How we work with the authorities? We talk about that event, we talk about what investments we made. And we heard from the last House committee from North Carolina discussing just that resiliency, that reliability, more deployables. So we are in discussions with the Authority right now to make those investments for the deployable program.

Senator BUDD. Yes. Thank you very much. And I think most of those 89 requests were from me. So appreciate your patience.

Mr. ADKINSON. OK.

Senator BUDD. A similar question, Mr. Davis. What takeaways from Helene did Frontline have to inform the future investments? And did the fact that Frontline was available as an alternative first responder network, did that improve outcomes?

Mr. DAVIS. Yes, Senator, that is an important question. And it was great to see you and meet you at our event and rally a few months ago.

Senator BUDD. Yes.

Mr. DAVIS. I know the team really appreciated and so did the community.

Senator BUDD. Yes.

Mr. DAVIS. I will tell you this, Senator, I was boots on the ground about 72 hours after Helene hit. And like my colleagues at AT&T, we had hundreds of requests coming in from seven different states. I spent time in Bunkham County and the EOC. I spent time in the EOCs in Asheville. And I spent time with law enforcement who were pulling bodies out of the mud and did not have any network capabilities, while we were trying to facilitate drone missions to provide these flying, thinking about flying towers in, literally, the middle of nowhere.

And then working with the Army Corps of Engineers to get radio equipment up on Mitchell Mountain because it was completely wiped away.

The lessons learned was around communications and partnerships and how important it is to have that streamlined communication, and it really is—and we are so proud to serve, on the primary side, nearly 52 percent of your constituents, Senator Budd.

And the other thing that we have learned is how important it is to do, you know, what you heard here with the hotwash, we call them after-action reviews. We did one internally on how we can do better, but we also do that with your local agencies as well. That way we maintain that continuity, and we maintain that communication throughout, and God forbid that there is another storm, but if there is one like Helene we will be ready and more prepared than ever.

Senator BUDD. Fantastic. Chair, thank you.

Senator FISCHER. Thank you Senator Budd.

Senator Klobuchar, you are recognized.

Senator KLOBUCHAR. Thank you very much, Madam Chair.

We have had a lot of tragedies in my state this year but one of them that I didn't discuss earlier was the murder of Melissa Hortman and her husband. And it is relevant here because there was a manhunt, like no other, in our state that went on for days. And the first responders were able to rely on FirstNet to communicate. They did find the now defendant and he was not able to kill anyone else, despite shooting another legislator and his wife 15 times, and going to several other houses.

Mr. Maier, what metrics do you believe that FirstNet should rely on to evaluate network performance and reliability and—why don't you answer that?

Mr. MAIER. I would like to note, and say thank you for your support for Next Generation 911 and everything that you do to help us.

Senator KLOBUCHAR. Yes.

Mr. MAIER. Operational performance under stress, that is what we are talking about. The public safety has to have the tools they need during the crisis. Latency, when we are talking about voice, push-to-talk setup, video delays, the packets. Are the packets moving through so mapping and AVL can get the job done, throughput, uplink, downlink, we use uplink in the field, first responders use uplink more than they do the downlink for sending data back.

We look at cell edge performance, on the edges of those maps where they say that there is coverage, is it actually performing, the priority activation times, the preemption metrics, those are important. Are they working?

We also look at quality of service. We look at the times when—how are these things moving forward? I also have mentioned before, power backups, are these batteries? Are these generators? Are they moving forward? And think about cyber security. Are we doing everything we can to keep the network safe? Are we introducing new vectors?

Senator KLOBUCHAR. Thank you.

Mr. MAIER. Thank you, ma'am.

Senator KLOBUCHAR. Thank you. You noted, I actually co-chair the 9-1-1 Caucus with Senator Budd, and we have introduced legislation to update some of these outdated centers, the related technology, the fact that everyone is using text messages. And this is all when I was the DA County Attorney for our biggest county we had, not in my county, but another one, there was a horrible shooting of a police officer, and that was when we realized that the responders to the scene tracking down the killer were—had 10 different radio. It was a mess. And that is what made our state, at least in the metros, the counties got all on the same network, and we have greatly improved things.

But now, you know, we are in this next moment where we have to look at the new technology and get there. So in your testimony you said that FirstNet should provide network coverage to even the smallest of the small emergency community centers, communication centers. Do you agree that updating our 911 centers is critical?

Mr. MAIER. It is, ma'am.

Senator KLOBUCHAR. And can you talk about how first responders, how important it is for them to have this kind of information, especially when they are in smaller rural areas?

Mr. MAIER. It is information, it is situational awareness. It protects the responders and it also protects the callers. We need that information into the 911 centers through the best ways possible. Those can include answering the call, getting the metrics, getting the information, getting all that, but then what do we do with it? How do we share it? Having those IP networks, those Next Generation 911 technologies interfacing with FirstNet, gets the job done.

Senator KLOBUCHAR. Thank you. Mr. Agnew, do you want to just talk about that rural issue and how broadband, as you know, the BEAD money, we have recently got some of that, that has been announced is going to go out, and talk about what steps AT&T does to ensure that rural communities are covered under the FirstNet network?

Mr. AGNEW. Absolutely. And thank you for that question. So as part of the opt-in process, so each state had to select FirstNet, they could have—choose to build their own network, each state and each territory chose to do that. As part of that process, 1,200 sites were built, not based off of AT&T selecting, it was based off of the voice of public safety. So that further expanded the network.

Also, as part of the obligation of the FirstNet contract, 15 percent of the network had to be built with rural partners. So states like Nebraska and other rural states received more than 2,000 loca-

tions. Their tribal lands grew by 66 percent in coverage. There are tribes in this Nation that are making phone calls for the first time. And then of course with the addition of the investment from FirstNet, they just approved an additional 137 sites based specifically off of public safety feedback.

Senator KLOBUCHAR. Um-hum.

Mr. AGNEW. States like California, states like Kentucky, states like Alaska, Hawaii, all states being addressed based off of feedback. So that is what is making a difference. It is not the carrier building a network, the carrier is building the network as the contractor, but it is Public Safety's decisions, and that is controlled by Sheriff Adkinson, and his Board, and the FirstNet Authority directing AT&T to develop that.

Senator KLOBUCHAR. OK. Thanks.

Sheriff, if you want to add anything. Then I will be done.

Mr. ADKINSON. Yes, ma'am. I think that can be part of an uncomfortable conversation sometime, right? Because the reality is, it is not based on the commercial market, it is based on what is best interest of the people we serve. I am not going to suggest that it is perfect. I suggest it is getting there every day. And so I think by making these investments in rural and tribal areas, this is at the heart of what we should be about. It is at the heart of what FirstNet is about, that all people, all public safety, and all the citizens are entitled to these communications.

Senator KLOBUCHAR. Um-hum. Yes. Because the market probably wouldn't dictate a remote snowmobile trailer.

Mr. ADKINSON. Sure. If a building—

Senator KLOBUCHAR. In Minnesota where they are—they break down and they are in the middle of nowhere, and they have to be able to call in, so just to say that—

Mr. ADKINSON. And it is a consistent need.

Senator KLOBUCHAR.—that happens quite often, but I am not going to go on. So thank you. And thank you to you, Mr. Davis, as well. Thank you.

Senator FISCHER. Thank you, Senator Klobuchar.

Building off of Senator Klobuchar's first question, Sheriff Adkinson, the Commerce Department Inspector General previously found gaps in the Board's oversight of performance metrics and milestones of FirstNet. FirstNet's initial response even challenged the IG's findings, asserting they were just working goals and not quantifiable metrics. So what new performance standards or monitoring methods has the Board approved so that we can ensure compliance with contract terms and with the law?

Mr. ADKINSON. Thank you, Senator, for that question. As I stated before, there are six new Board Members, correct, that just came on this last October. And the first thing we did was go back through these Inspector General reports. There are obviously also three permanent members that provide oversight to the Board which is OMB, the Department of Justice, and Department of Homeland Security, who are also obviously permanent members of that.

We, as a Board, started saying what performance measures matter, what performance measures are actual returns on investment and started a working group to do that to make sure that those

things are being—monitor those things that matter and we start asking some tough questions. I want to talk about OIG specifically, because I think this is important.

You know, if you want to have accountability, you have to have authority. And I am not a real fan of not being able to hold people that I give directions to accountable because otherwise I am simply suggesting. And I don't like suggesting, if I am being blunt. I think there is a responsibility as tax stewards of the taxpayers' authority and money, these are taxpayers' funds in my opinion, that we, as a Board, should be able to hold the executive director and/or the Authority staff accountable as appropriate. There has to be some level of accountability.

Senator FISCHER. You mentioned that in your opening comments about—when you were talking about changes—

Mr. ADKINSON. Sure.

Senator FISCHER.—as we reauthorize FirstNet. Could you give us—wrap it up here? Senator Luján is going to have one more question, or more than one, as we wait to see if other senators are coming, but can you hit those points for us again at the end?

Mr. ADKINSON. Yes, ma'am. I want to make sure I answer your question correctly, all three points in that regard really quick. Yes, absolutely. So first and foremost, I think there should be an expansion of the public safety seats on the Board so that we don't lose what is the tenor and direction of what this Board should be about. It is looking after the interest of public safety, and making sure that doesn't become a secondary interest.

And I think that should be codified, to the staggering of terms so that we don't end up in a situation—you know, again we have six new board members plus two current vacancies, and I am actually just the acting chair at this point. Those are the kind of things that we need to give the Secretary of Department of Commerce the opportunity to make those corrections as appropriate. And I think that helps for continuity and consistency in government.

Three, which is too many captains on the ship. We have to have the ability to make decisions that matter and hold accountable. If you are going to ask me to be accountable I suggest that I need the authority to do that. And there are some clear things that I think we can go back that I can give you examples of where that was challenging.

Senator FISCHER. As you look at the current statute, do you think that the performance benchmarks and device connection targets are being met?

Mr. ADKINSON. I think there should be stricter, more outlined and more defined performance measures, that is in the best interest of the people we serve. Quite frankly, it is in the best interest of AT&T. Nobody loses with us being more accountable and having performance measures. It is the right thing to do.

Senator FISCHER. Thank you, sir.

Senator Luján.

Senator LUJÁN. Thank you, Madam Chair. Good questions.

Mr. Agnew, what is FirstNet's presence in rural, tribal, and remote areas of New Mexico, and is coverage there truly sufficient?

Mr. AGNEW. Thank you for that question, Senator. We need continued buildout. While New Mexico has received significant build-

out for the FirstNet program, there is more work that needs to be done, and there is a couple things that are being done. As I mentioned, the coverage workshops where new sites are going to be built based off of your first responders. Additionally, we make available deployables so they can pull out their own coverage. We make it highly affordable, small form factor so they can deploy coverage where it doesn't exist.

Finally, as I mentioned before, the partnership with AST that is going to fill out much of the white space that is in Nebraska—or sorry—New Mexico, I apologize. And that is where we are going to be able to provide a layered approach to deliver that connectivity for New Mexico.

Senator LUJÁN. Mr. Agnew, if you don't have the percentage of the state that is covered or where the holes are, you could just respond to that one in writing. New Mexico is one of the first states that adopted into FirstNet, and if I am not mistaken, we were one of the early adopters.

Mr. AGNEW. Yes, sir.

Senator LUJÁN. We still have holes, man. I can tell you, where I drive where phones don't work. And I have got them all.

Mr. AGNEW. Right.

Senator LUJÁN. And when I talk to local law enforcement agencies, you know, some of my CDS comes from trying to help local law enforcement agencies, there is a fire chief that lives in a canyon and once he gets past a certain mile marker, you can't find him. You cannot find him. You can't even bounce off of radios to get to this this family. And this is in a mountainous area where a little fire kills people, devastates homes.

And so I am really interested here. And you know, with that being said, I would be happy to work with the Chair to look at the holes that exist across America in rural communities, and so that we can just get a better understanding of success, measuring success every year that we deploy, how we do better.

Mr. Davis, same question to you.

Mr. DAVIS. Yes, Senator, that is a great question. And, I will tell you, we are we are proud to support nearly 61 percent of the first responders in New Mexico. I know those challenges very well. I actually have a home in Northern New Mexico, and spend a lot of time there.

You know, some of the things that we are doing we are doing a lot of the similar things, and I think what is important to understand here at the end of the day there is no separate network, there is no separate commercial, there is one commercial truck carrier that is providing these services for public safety, there are multiple carriers that are doing that today. I think that is important, that is why we are here.

So if FirstNet is getting funding, we are looking at additional \$15 billion over the next, you know, 25 years of the term, and they are to put a tower in that canyon, that tower should be able to cover all the public safety providers, not just AT&T customers, because what we have seen in national outages, and what we have seen in recent times, is when there is an AT&T outage, FirstNet is out too.

So there is no separate network and there is no—everything is riding on AT&T's commercial network. And I think that we—that

is a good reminder for us, and a good reminder for rural coverage that we all have to work together, and that is why it is important that we have competition in the marketplace.

Senator LUJÁN. Mr. Agnew, let me ask you a question that I presented earlier. Does technology exist today where, if a first responder buys a phone, a communication device, can they ride all three networks with subscriptions? Or do they have to buy a phone from each—from each carrier?

Mr. AGNEW. So thank you for that question, Senator. Today, the technology does exist where phones can use multiple SIM cards from carriers as well as routers.

Senator LUJÁN. But do they have to change a SIM card out or does it just work?

Mr. AGNEW. There is, two options that the routers just work, the SIM cards there is a—there is a configuration but it is very simple to do, and it is very standard from a public safety perspective to have multiple SIMs within a specific device.

Senator LUJÁN. Sheriff, I am clearly talking about something I don't understand, because I see several heads in the room nodding, either against me or with Mr. Agnew here, if you will. Is this widely known? Are we seeing agencies across the country rather—because look, when I am back home and I am talking to folks, they are rolling with three, four phones, right. And is this widely known, because it sounds like it could be a savings?

Mr. ADKINSON. Well, I have got three phones, so I am not sure how that helps. No, I mean, pragmatically, yes, it is widely known.

Senator LUJÁN. Yes.

Mr. ADKINSON. It is well known. And it is not uncommon for agencies, when you hear these folks talking about the number of agencies, 40,000, we have got 30,000 a well, you know, maybe my math is not that good, but there is a limited number of public safety agencies in this country, right?

Senator LUJÁN. Um-hum.

Mr. ADKINSON. The reality of, is many organizations use multiple lines based on what is in their best need. And you are never going to hear the Authority, the Board tell somebody to go away from a service if they are not able to provide it yet.

Senator LUJÁN. Yes. Um-hum.

Mr. ADKINSON. I don't want—Russo (sic) said it perfect, right, which is "Don't let perfect be the enemy of better". We are getting there, but we are not going to endanger somebody's life by telling you to drop your service when we are not providing adequate service yet. The goal is to get to providing adequate service. But to your major point, it is not uncommon for people to use multiple lines.

Senator LUJÁN. Amen to that. Last question that I—well, my time has expired here, so please respond. Just, a follow up that I have is if you could respond to me, both Mr. Agnew and Mr. Davis, is if law enforcement knows that there is a hole somewhere and they have a subscription to either of you, what do they do to report to you all that there is a hole?

Side by side to that, if I have a constituent that goes and buys a phone based on the maps that you all presented, and the phone don't work, what do they need to do to respond to the company to

say, hey, the map said I have got coverage here. I don't have coverage. You need to fix this. So if you all could respond to that?

Mr. AGNEW. Sure. Very quickly, that direct relationships between the FirstNet consultants and your public safety agencies that there is a direct relationship there to report the coverage, also with the FirstNet Authority and those covered workshops to document it, and then we subsequently provide updates.

We are accountable. We are bound by the contract to provide those updates. We are bound by the contract to provide that build-out plan. So it is full awareness. And if there is any public safety officials in your state that are not aware of that, please, please let them know that it is available to them.

Senator LUJÁN. I appreciate that.

Madam Chair, I am reminded of that app that the FCC created when they were trying to fix these maps that were horrible. I used it a time or two when devices weren't working. I just don't know if something equivalent exists or still exists for the others. So, that is what I am looking at, to try to help more folks. Yes.

Senator FISCHER. Yes. I am with you on that. In fact, I was going to follow up with it before I recognize Senator Sullivan. On the maps that are available to the FCC and to the public at large, I would just ask each of you, yes or no, are they worth anything?

Go ahead, Sheriff.

Mr. ADKINSON. Absolutely. It is going to show you the overall, right, how good in particular that coverage is, that is questionable, right. I think that is always something that could be improved. I am kind of a trust, but verify individual when it comes to that. So that is an individual.

Senator FISCHER. There you go. Mr. Agnew?

Mr. AGNEW. It provides directional coverage, but with FirstNet, we actually provide much different layers that actually show in-building, outdoor, more specificity before a first responder comes on. So there is much more that a public safety—

Senator FISCHER. So FirstNet is—which we have already established, is more reliable than your commercial service?

Mr. AGNEW. That is right. With the priority preemption, correct?

Senator FISCHER. Thank you. Mr. Davis?

Mr. DAVIS. The answer is yes, but I think there is still more, more work to do.

Senator FISCHER. Yes. Thank you. Mr. Maier?

Mr. MAIER. We call that drive testing in the field. You go out and you check, and you verify. I do want to note that for Senator Luján, I have a phone here that has two SIMs in it. One on one carrier, one on the other. And if I could put three on it, I would use all three. Get one device, sir.

Mr. DAVIS. Can I have 30 seconds to respond to that? I think it is important. That is why we are here, right. There is going to be \$15 billion going to the FirstNet Authority over the next 25 years. There is a lot of rural departments, Taos, New Mexico, for example, that can't afford two SIMs. It would be great if that money went back to the public safety agencies, instead of going to one commercial provider to build out their network.

Senator FISCHER. Thank you, Mr. Davis. I think Senator Luján and I should do road trips in New Mexico, and then he comes to

Nebraska and we will do it in Nebraska, and we will include Alaska in this——

Senator LUJÁN. That is my home.

Senator FISCHER.—as we travel our very sparsely populated areas of the state, and we can tell you exactly where we can do calls. Thank you.

Senator Sullivan, you are recognized.

**STATEMENT OF HON. DAN SULLIVAN,
U.S. SENATOR FROM ALASKA**

Senator SULLIVAN. Thank you, Madam Chair. You are always welcome to Alaska, as you know.

And I want to—I want to thank the witnesses. It is a really important topic. And I want to thank the Chair and Ranking Member for holding this hearing.

So I want to talk a little bit about lessons learned on the issues of really remote areas, like my state, like the Ranking Member's and the Chair's state, and what we learned from the Maui wildfires, because I think there are a lot of lessons learned. So you know, my state, the Great State of Alaska, has benefited from meaningful FirstNet investments, and strong response efforts by AT&T and FirstNet response operations groups.

But I think the Maui wildfires show that plans and assets must be demonstrably ready before a disaster occurs, especially in remote challenging regions of the country. And I would like all the witnesses' views on this. Do you agree that for remote states, but I guess it is really for all states, but in particularly remote big states like mine, that the public safety, communications, disaster recovery plans must be proven through exercises and logistics testing, not just written commitments. Because I think what happened in Maui is you had all these great written commitments, but there was nothing that was Hawaii-specific in the protocols.

And I am now looking at the OIG Report that came out, and that the FirstNet Authority approved AT&T's Business Continuity and Disaster Recovery Plan just 2 months before the Maui wildfires, and yet that plan failed miserably, I think.

So can I get everybody's view on that? It is a really important issue. Don't just have a written plan. Hey, this looks good. You have got to go test it, especially in a place like my state, very remote, very rugged. What is the view on, yes, from all the witnesses? And then what can we—you know that was just such a horrible tragedy in Maui, my God, but you know, what is the silver lining on lessons learned from that? Because I think there is a bunch in the OIG Report certainly has some——

Mr. AGNEW. So Senator——

Senator SULLIVAN. I will leave it up to you then, all four of you.

Mr. AGNEW. Yes, Senator, thank you. And you are right, it was a tragedy. And let me just start with saying oversight is good for the program. It drives continued growth and innovation so we meet public safety's needs, and FirstNet is really the only provider with this healthy oversight, and is contractually bound to deliver for public safety.

So let us talk about learnings. I have been to your state. I have performed public safety exercises in your state, Juneau, Alaska;

Anchorage, Alaska, working with public safety. I personally know——

Senator SULLIVAN. And by the way, just really quick, those are the big populated areas.

Mr. AGNEW. Right, of course.

Senator SULLIVAN. We had a typhoon that smashed into Western Alaska a few months ago in these remote villages on the western part of our state that—and that is where I really want you to be doing.

Mr. AGNEW. Right.

Senator SULLIVAN. I want you doing exercise in Juneau and Anchorage, don't get me wrong, but I want you to be doing exercises in some of the most remote parts of America that have been really severely impacted by extreme weather.

Mr. AGNEW. So to that end, you made a commentary, you are so far from the mainland, so you have to be self-sufficient. So the business continuity and disaster recovery plans, and the resources, you have to be able to self-sustain before the cavalry comes.

We take the OIG Report very seriously. It is that roadmap for improvement. So let us focus on Maui. Maui had a device, had it deployable onsite, was deployed within 24 hours. We have subsequently sent 30 devices, but what I said was subsequently sent, right. It needs to withstand now.

So what we have done is we have tripled the amount of assets on each of the islands. So now, we can respond much faster. We have coordinated with National Guard and the Hawaii Emergency—EOC, to receive priority on barges and airlift, so if deployables need to move between the islands.

From an Alaska perspective, because that learning didn't just stop at Hawaii, it is now the territories, it is U.S. Virgin Islands, it is Puerto Rico, it is Alaska, where we have to operate differently and deploy more assets. So we have actually doubled the assets in Alaska and continuing. We are updating, and we will continue to update our business continuity disaster recovery plans to continue to show what we are doing there.

But to answer your question directly about testing it, not just putting on paper.

Senator SULLIVAN. Yes.

Mr. AGNEW. Yes. And that is why we have a dedicated ROG Team with that specific responsibility to coordinate with your state. This is Alaska, this is Hawaii, this is North Carolina, this is New Mexico, and Nebraska, we are required to coordinate that effort. So thank you.

Senator SULLIVAN. Good. That is a good answer. Anyone else have a view on that? I am sure you all do, but it is a really important question.

Mr. DAVIS. Yes. A very important question, Senator. And the tragedy in Maui was just devastating. And this is exactly why we are here, and exactly why the reliance on a single network provider is a risk to public safety, and something that we just cannot afford. So you know, from our perspective, the only true service of last resort is redundancy.

Senator SULLIVAN. Yes.

Mr. DAVIS. So disaster plans must be tested physically, not just contractually. You know, our contract is with our network and our customers, not a Federal mandate. But more importantly, public safety agencies need access to multiple networks. If the primary network fails, whether due to a wildfire, or a fiber cut, or a cyberattack, Alaska's first responders need to be able to immediately switch to another carrier.

Senator SULLIVAN. Good. And by the way, you know my state, we get a lot of natural disasters, right. Earthquakes, wildfires, tsunamis, you name it, we get them. So it is really important. Any other thoughts on this? I know I am over time, but it is an important question.

Mr. MAIER. Just a short note to say that networks, when they are overloaded, damaged, or simply unavailable, it is a problem. First responders have to communicate with each other and communicate with the public. And we believe at APCO International, our members do this every day, is that we plan. We plan with redundancies. We have multiple ways to communicate.

These may be land mobile radios, it may be high-frequency radios, it could be multiple carriers, a mix of technologies that really is field tested. You talked about scenarios. scenarios exist today that you can tabletop about how do they work in the field?

Senator SULLIVAN. Yes.

Mr. MAIER. Allow the first responders to work out in the field to find those gaps, identify them, make corrections, you will have successful—more successful outcomes.

Senator SULLIVAN. Good. Sheriff, do you have a—do you want to wrap it up here?

Mr. ADKINSON. Yes, sir. You know, unfortunately, the State of Florida handles its fair share of natural disasters as well, too. And one of the things that we know and have learned, that I think the Authority, as a Board, is pushing for is this concept of critical complement, which is what needs to be done after these after-action reports. (A) Is it predictable? If it is predictable, it is preventable, right?

Senator SULLIVAN. Yes.

Mr. ADKINSON. (B) Is it a practical application of resources where it is at? So we can have all the resources in the world, but if they are only in D.C., they are not doing anybody any good. So I think what we have learned as we step up these after-action reports is that there has to be a critical—at least a critical complement for all areas of the country. I think that is a buildout process. I am not going to tell you it is perfect today, because it is not. But that is part and parcel of learning from these national disasters.

Senator SULLIVAN. Great. Thank you. Thank you.

Thank you, Madam Chair.

Senator FISCHER. Thank you, Senator Sullivan. And thank you to all of our witnesses for their testimony here today. Senator Luján, thank you, and I look forward to working with you and with all of our colleagues to work together on this important issue as we look forward to the reauthorization of FirstNet.

Senators will have until the close of business on February 4 to submit questions for the record. The witnesses will have until the close of business on February 18 to respond to those questions.

This concludes today's hearing. And with that, the Committee stands adjourned.

[Whereupon, at 11:27 a.m., the hearing was adjourned.]

A P P E N D I X

NATIONAL SHERIFFS ASSOCIATION
MAJOR CITIES CHIEFS ASSOCIATION
January 21, 2026

Hon. TED CRUZ, Chairman,
Hon. MARIA CANTWELL, Ranking Member,
Senate Committee on Commerce, Science, and Transportation,
Washington, DC.

Dear Chairman and Ranking Member,

As your committee considers reauthorization legislation for the FirstNet Authority (FNA) prior to 2027, we urge you to consider critical updates that will improve the effectiveness of the program through enhanced oversight, accountability, competition, and transparency regarding the billions of dollars that it spends. To be clear, we strongly support the FirstNet concept and seek to improve its structure. Our primary objective in seeking these changes is to ensure that the FirstNet Authority is working to the benefit of *all* public-safety users.

Congress's original vision of FirstNet, a standalone, publicly-owned network exclusively for public safety use, was laudable. The reality of the effectiveness of this model is now apparent: it has not worked as envisioned. The reauthorization process represents an opportunity to improve this critical program.

First, it is imperative that any reauthorization measure does not permanently extend the FirstNet mandate. As we have seen over the past decade, technology and the needs of the public safety community have evolved dramatically. FirstNet should be revisited and updated over time, not put on a permanent autopilot. We urge that FirstNet's reauthorization remain on a Congressionally mandated cycle.

Second, we urge the Congress to ensure that the FirstNet program benefit all of public safety, not just the customers of a single commercial carrier. The fact that all of the FirstNet Authority's multi-billion-dollar spending has gone to only one single carrier, AT&T, has been exposed as problematic in recent years. When the AT&T network went down in February of 2024, AT&T's FirstNet customers lost service. This is a risk our first responders simply cannot take. They need consistency and reliability for their communications networks. Many of our members now depend on multiple carriers to ensure reliability and resiliency. In the years since FirstNet's contract was awarded to AT&T, other carriers have developed their own public safety offerings. This competition has resulted in a better product for our public safety users. Congress should ensure that all infrastructure paid for with FNA funds is being used to the benefit of all public safety users, not just the customers of a single carrier.

Accountability must also be prioritized in the new reauthorization measure. In recent years, the Inspector General for the Department of Commerce has issued multiple reports highlighting a lack of transparency and accountability within FirstNet and particularly with regard to AT&T's compliance with the FirstNet contract, including accusations that requested data was altered or not provided. This is unacceptable. To this end, we urge policymakers to include enhanced reporting and accountability requirements in the reauthorization measure, including:

- Reporting on the use and capacity of Band 14.
- Providing a full range and categorization of FirstNet subscribers including public safety, fire, EMS, private companies, etc.
- Disallow the use of government funds to support contractors, events, and marketing for any carrier.

Finally, we urge that policymakers include a provision that repeals grant/procurement requirements that favors AT&T given its exclusive partnership with FirstNet. This practice is outdated given the advancement of public safety communications

options, and ultimately benefits a single corporate entity, not the public safety community.

As previously stated, our goal in making these recommendations is developing a stronger, more resilient public safety communications network. We believe that the experience of the past decade makes clear that changes must be made.

Sincerely,

JEFF NORMAN,
Milwaukee Police Department,
President,
Major Cities Chiefs Association.

SHERIFF CHRIS WEST,
Canadian County, OK,
President,
National Sheriffs' Association.

CC: The Honorable Deb Fischer, Chairman, Senate Committee on Commerce, Science, and Transportation Subcommittee on Telecommunications and Media

The Honorable Ben Ray Lujan, Ranking Member, Senate Committee on Commerce, Science, and Transportation Subcommittee on Telecommunications and Media

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DAN SULLIVAN TO
MICHAEL A. ADKINSON, JR.

Disaster Recovery Plan Approval Standards:

The OIG found that FirstNet Authority approved AT&T's Business Continuity and Disaster Recovery Plan on May 30, 2023, just two months before the Maui wildfires, even though the plan did not demonstrate the ability to restore service within required timeframes and did not include Hawaii-specific protocols. Alaska faces similar challenges—remote communities, limited transportation options, and frequent natural disasters—making region-specific, proven recovery planning essential.

Question 1. What specific objective standards does FirstNet Authority use to approve a disaster recovery plan, and why were those standards met in this case despite the plan's failure during a real-world disaster?

Answer. As outlined in the FirstNet contract requirements, the plan comprehensively addresses:

- Written disaster recovery plans for all critical technology and infrastructure, including the Nationwide Public Safety Broadband Network (NPSBN).
- Proper risk controls to ensure continued performance of the contract in the event of a disaster.
- Procedures that will be invoked in the occurrence of a Force Majeure event.
- Demonstrated capability to provide uninterrupted access to the NPSBN during the disaster within the recovery time objectives.

The Board ensures that the FirstNet Authority management continually executes oversight of its contractor, AT&T, to ensure contract requirements are met while also implementing corrective actions when performance measures are not being met. To be frank, we can do better. We will continue to process lessons learned and make investments and improvements to ensure contractual obligations are met and public safety's unique critical communications needs are addressed. The Board stands ready to work with Congress during reauthorization to provide additional tools to enhance oversight of the contract and set public safety up for success for the next ten years.

Question 2. Why isn't approval of a FirstNet disaster recovery plan contingent on regular, documented, live exercises that prove deployable equipment can actually be activated and deployed on time?

Answer. The Board has directed the FirstNet Authority management to actively exercise oversight of disaster recovery through live demonstrations and testing of the deployable service. Between 2023 and 2026, the FirstNet Authority conducted comprehensive live exercises in diverse and challenging environments, including, Alaska (Girdwood), Puerto Rico (San Juan and Aguas Buenas), the Northern Mariana Islands, American Samoa, and the U.S. Virgin Islands. A future verification event is planned for Hawaii as part of the Maui Action Plan implementation in March 2026.

By contract, AT&T is required to submit formal test reports twice annually, ensuring accountability and performance tracking. As we continue to strengthen the rigor of our process, the Board is committed to ensuring the integration of existing oversight of deployable assets with the Disaster Recovery Plan framework. Creating a direct link between operational testing and documented recovery strategies enhances resiliency, validates readiness, and ensures alignment with contractual and industry best practices.

Question 3. Does FirstNet require disaster recovery plans to be validated through logistics exercises—such as actually moving equipment to remote or island locations—and if not, why?

Answer. Between 2023 and 2026, the FirstNet Authority conducted comprehensive live exercises in diverse and challenging environments, including, Alaska (Girdwood), Puerto Rico (San Juan and Aguas Buenas), the Northern Mariana Islands, American Samoa, and the U.S. Virgin Islands and is actively working to evolve this process into a fully integrated component of the Disaster Recovery Plan. By connecting operational testing with documented recovery strategies, we aim to create a seamless oversight model that validates readiness and strengthens resilience. This continuous improvement approach ensures that lessons learned from live demonstrations directly inform and enhance disaster recovery planning.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. MARIA CANTWELL TO
MICHAEL A. ADKINSON, JR.

Outstanding GAO and OIG Recommendations. The Government Accountability Office and the Department of Commerce’s Inspector General released a number of extremely troubling reports that have raised serious concerns about a troubling pattern: when AT&T falls short of its contractual requirements, the response has been to change how performance is measured rather than to actually improve performance.

When AT&T failed to meet FirstNet adoption requirements in 34 states, the Authority replaced strict state-by-state standards with a nationwide average—a change AT&T itself proposed—allowing \$38 million in penalties to be waived. When AT&T was on track to miss deployment targets in rural communities, the Authority changed how deployment was calculated, helping AT&T avoid penalties and collect additional payments.

And with the Maui wildfires, the OIG found that AT&T altered data after the fact. AT&T downgraded requests for temporary cell sites from requiring immediate action to a lower priority. The report documented staff comments about “backdating” request times and needing to “pad my stats.” The FirstNet Authority failed to catch this until the Inspector General brought it to their attention.

Question 1. Sheriff Adkinson, will you commit to holding AT&T responsible for altering data or providing inaccurate information to the FirstNet Authority, and to reject attempts to modify the contract to weaken performance standards?

Answer. Yes. As I testified regarding issues raised by the Department of Commerce Office of Inspector General (OIG), the Board, NTIA, and FirstNet Authority management are fully committed to ensuring the best possible network for public safety. That includes ensuring that our contractor AT&T performs its contractual obligations. A cornerstone of the success of FirstNet’s contract is the unique transparency and accountability to public safety and oversight by the OIG, other government auditing bodies, and members of this Committee. Of course, it is also clear that we can do better, and reauthorization is a key opportunity for Congress to give us the tools we need to set public safety up for success for the next ten years.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. BRIAN SCHATZ TO
MICHAEL A. ADKINSON, JR.

Question 1. In December 2024, the Department of Commerce Office of Inspector General issued a report, “Nationwide Public Safety Broadband Network Was Not Always Available to First Responders During the Catastrophic 2023 Maui Wildfires.” What is the status of FirstNet Authority’s compliance with, and implementation of, the eleven recommendations from the report?

Answer. FirstNet Authority has fully implemented 9 of the 11 Recommendations.

a. What is the status of any pending recommendations?

Answer. Of the 9 recommendations implemented, 3 recommendations have been accepted by the OIG for closure (*i.e.*, recommended steps have been satisfactorily

completed), and 6 recommendations are being reviewed presently by the OIG for closure.

b. When can you guarantee these recommendations will be fully implemented?

Answer. Work on the remaining 2 recommendations is in progress now and targeted for closure within FY 2026.

Question 2. Why did FirstNet Authority approve AT&T's business continuity and disaster recovery plan, which incorrectly included Hawaii in its plan for the continental United States?

Answer. The Business Continuity and Disaster Recovery Plan is a Network based plan that is tailored to the Network Operator. This plan covers all states where AT&T is the network operator, including Hawaii. At the time of approval, the FirstNet Authority determined that the baseline plan met contractual requirements. Since the after-action review and lessons learned from the Maui incident, the Authority has been working to strengthen the plan. The new plan requires further detail and rigor and we are committed to continual improvement of the plan. Additionally, to strengthen oversight and improve quality, management has since expanded the review team by assigning additional subject matter expert resources, ensuring broader expertise and more rigorous evaluation to strengthen the oversight of the program and our disaster recovery efforts.

a. What oversight and approval protocol was in place at the time of FirstNet Authority's approval of the plan? What specific gaps contributed to this error?

Answer. FirstNet Authority utilized a structured Deliverable Review Process to ensure quality and compliance across all submissions. This process has improved over time by addressing resource gaps—adding subject matter experts and reviewers to manage the high volume of deliverables effectively. Following the Maui incident, AT&T has deployed fourteen new assets across the Hawaiian Islands of Hawaii, Kauai, Maui, and Oahu. Hawaii's new deployable assets include four Compact Rapid Deployables (CRDs), six miniCRDs and four Low-earth orbit Emergency Communication Portables (LECPs). CRDs provide up to two miles of portable FirstNet coverage without relying on external power sources. MiniCRDs can be transported as checked luggage and deliver up to half a mile of coverage for emergency operations. LECPs use low-earth orbit satellite links to restore communication when fiber or microwave connections are unavailable. With the addition of the new deployable assets, the number of locally available FirstNet deployable assets in Hawaii was tripled.

b. What changes has FirstNet Authority made to address these oversight and approval errors?

Answer. The FirstNet Authority performed a concentrated review of the Disaster Recovery Plan as part of its implementation of the Maui Audit Recommendations. To improve our oversight and address errors, we added additional reviewers to obtain a wider scope of subject matter expertise. Following this exercise, the FirstNet Authority held several engagement sessions with AT&T to clarify expectations. The Authority now has an updated Disaster Recovery Plan with an Appendix specific to the Nationwide Public Safety Broadband Network, which provides greater traceability to our contract requirements.

c. Did FirstNet Authority previously confirm whether Hawaii state public safety officials were involved in the development and approval of the business continuity and disaster plan?

Answer. The Business Continuity and Disaster Recovery Plan is a network-based plan that is tailored to the network operator. In the case of the Continental United States, Hawaii, and Alaska, AT&T is the network operator.

Previously, states were invited by AT&T's Response Operations Group (ROG) to participate in a voluntary exercise to establish state specific response coordination plans. For Hawaii specifically, an initial engagement occurred, however the plan was not completed. The Board acknowledges the need to become more involved in the state specific planning process. As such, the Board has directed the FirstNet Authority Public Safety Advocacy team to engage directly with both AT&T and states to establish state specific response coordination plans. This exercise will update plans that were established under the voluntary process and will establish plans for states that didn't previously have them, including Hawaii.

d. Will FirstNet Authority now confirm the involvement of Hawaii state public safety officials in the development and approval of the new business continuity and disaster plan?

Answer. Yes. The Board will ensure the active involvement of Hawaii state public safety officials in both the development and approval of the Hawaii response coordination plans. These plans are designed to complement AT&T's nationwide Business

Continuity and Disaster Recovery Plan by incorporating localized requirements and operational realities. This coordinated approach ensures that national standards are reinforced with state-level strategies, delivering a more resilient and responsive framework for emergency preparedness.

Question 3. The first recommendation from the Office of the Inspector General report directs FirstNet to ensure that special hardening measures are implemented for the unique threats faced in the Maui region, as required by the NPSBN contract. What specific hardening measures have been taken to address this recommendation?

Answer. In addition to complete site and backhaul restoration, additional hardening measures include additional FirstNet cell sites, changes to vegetation/landscaping plans, increased generators (fixed and portable), an on-island technician and additional deployables to ensure capability on each island, and reduced reliance on the need to move large/heavy equipment between islands.

a. What other hardening and resiliency measures have been taken aside from deployables?

Answer. Following the fires, hardening and resiliency measures include: (1) site repair and replacement; (2) new sites added post-fire; (3) changes to landscaping plans; (4) increased number of sites with fixed generators; (5) installation of generator camlocks for expedited hook-up for temporary generators; (6) additional portable generators; and (7) on-island dedicated technicians.

b. Have additional hardening measures been adopted for other high-risk areas since the Office of the Inspector General report was released?

Answer. The FirstNet Authority included requirements for fixed generators for standard new site builds funded through our Coverage Enhancements reinvestment. The Board also recently approved an investment to upgrade the FirstNet core to support future public safety specific direct to device capabilities, which could serve as a backup in areas where terrestrial service is temporarily impaired.

c. Are additional hardening measures, aside from deployables, planned for other high-risk areas?

Answer. The Board views hardening measures as necessary to meet the required Nationwide Service Availability requirement of 99.99 percent. This calculation is based on network probes located throughout the country, including high risk areas. In addition to measures already adopted, the Board is working with the FirstNet Authority management to investigate additional hardening measures in high-risk areas. Examples include logistical contingencies with local and Federal partners to facilitate better deployment among the islands and direct-to-device technology, which will benefit FirstNet subscribers by providing connectivity for devices from space when terrestrial cellular networks are unavailable.

Question 4. The Office of the Inspector General report found that AT&T altered data it reported to FirstNet Authority regarding the Maui wildfire response, and that FirstNet Authority did not have access to AT&T's real time network data. What barriers prevented FirstNet Authority from conducting appropriate oversight of these performance metrics?

Answer. By contract, the FirstNet Authority receives the Deployables and Temporary Solutions report on a quarterly basis which presents a barrier to oversight. FirstNet Authority has previously had to invoke its right to audit AT&T records to gain access to the raw data upon which these reports are based. Frankly, this is unacceptable. Following the events in Lahaina, FirstNet Authority management requested time stamp data for questioned entries to correlate report data and support event reclassification. We are actively pursuing real/near real time data for deployable dispatches, outages, and network performance data and have begun these discussions with AT&T as part of our work to implement one of the Maui Audit Recommendations.

a. According to the report, AT&T downgraded first responders' requests for 14 deployables from "emergent" (requiring immediate action) to "urgent" (requiring action between 14 hours and 30 days). What was the effect of AT&T reclassifying these requests from "emergent" to "urgent" on Maui wildfire response efforts?

Answer. "Urgent" deployments were not included in the Response Time Objective (RTO) calculation whereas emergent deployments were. FirstNet Authority required AT&T to resubmit this report including explanations for each event classification and reclassification within the Maui wildfires to ensure proper reporting. The contract did not previously include definitions for event types. We have corrected this as noted in the response below to ensure alignment of performance requirements.

b. How is FirstNet Authority implementing new protocols to ensure that these errors do not happen again, and that data-sharing is transparent, accurate, and trustworthy?

Answer:

1. FirstNet Authority modified its contract with AT&T to add definitions for emergency events that contribute to the Recovery Time Objective (RTO) and Non-Emergency events that do not.
2. FirstNet Authority conducted an audit of AT&T deployable data, including system records.
3. FirstNet Authority implemented an enhanced manual surveillance process.
4. FirstNet Authority invested in a Data Discovery and Virtualization Tool and built a use case specific to deployment events to help identify anomalies across large volumes of data.
5. FirstNet Authority conducted on-site field surveillance of the Deployables program at planned events and by exercising the request process for field-specific deployments.

Question 5. The Office of the Inspector General report found that FirstNet Authority did not ensure that AT&T's After-Action Report for the Maui wildfires included sufficient information about lessons learned and process and protocol improvements to implement. This is a requirement of the NPSBN contract. Why did FirstNet Authority not ensure sufficient information was included in the report?

Answer. The After-Action Report included "Key Learnings, Actions, and Recommendations," which were also discussed during the After-Action Briefing. These learnings were largely related to the need for more deployables in Hawaii to support multiple incidents simultaneously.

Question 6. How are deployables tested and assessed for readiness, and what training and resources are offered to state and local public safety officials?

Answer. The deployable assets are owned, maintained and operated by AT&T. FirstNet Authority staff routinely conduct oversight visits of the deployable assets, including observations at storage locations and actual field deployments to observe readiness and programmatic compliance.

a. What is the frequency of the training provided to state and local public safety officials?

Answer. Deployables are operated solely by AT&T and their subcontractors. The FirstNet Authority Public Safety Advocacy office provides education and outreach on availability and best practices regarding deployables to public safety stakeholders through forums held locally as well as nationally. The information is also widely available on FirstNet's website, as well as AT&T's. Educational events are conducted numerous times per year.

Separate from the deployables available through the contract, state and local organizations may purchase their own customer-owned and maintained (COAM) deployables. Purchasing agencies can arrange COAM trainings directly from the manufacturer in addition to online training videos.

Question 7. How does FirstNet determine its metrics for deployment success?

Answer. The FirstNet Authority currently relies on a Key Performance Metric known as the Recovery Time Objective (RTO) to assess performance. During the execution of recommendations for the Maui Audit, management initiated a working group to review how to measure our program's success, including the establishment of new requirements for measuring deployables' performance, which we will incorporate into contract oversight.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN HICKENLOOPER TO
MICHAEL A. ADKINSON, JR.

Federal Labs. Colorado is home to many Federal labs which perform mission critical research, development, and testing to improve communications service. The First Responder Network Authority, the NTIA's Institute for Telecommunications Sciences (ITS), and NIST's Public Safety Communications Research Division within the Communications Technology Laboratory all call Boulder, Colorado their home. The FirstNet Authority's lab in Boulder tests public safety technologies which will be used by first responders. NTIA's ITS lab is the gold standard for researching how to maximize spectrum efficiency and reduce interference to Federal agency missions and commercial radiofrequency applications. NIST's PSCR Division supports the de-

velopment of technical specifications to advance next-generation communications technologies.

Question 1. Do you believe the research activities performed by the NIST, NTIA, and FirstNet Authority Labs are key to the success of advancing the state of the art in public safety communications? Which areas of research or technical challenges in public safety communications may be useful to examine going forward?

Answer. The work done over the last 10 years by the FirstNet Authority, NTIA's Institute for Telecommunication Sciences, and NIST has spurred academic research and private sector innovation in public safety communications technologies worldwide. The FirstNet Authority's Boulder Lab demonstrates and verifies location-based services and mission critical service capabilities on the FirstNet network, enabling the FirstNet Authority to provide detailed and timely feedback on the public safety user experience.

The FirstNet Authority (through our network reinvestments) and NIST are both actively working to identify and support addressing gaps in key public safety communications technology and capabilities. This includes enhancing Mission Critical Push-to-Talk to provide a common operating picture through integration with computer aided dispatch (CAD), wearables, communications in austere environments (e.g., satellite and deployables) and the ability to communicate with no network infrastructure (device-to-device). Another is location services, especially related to tracking indoor first responder locations including in the vertical axis, and the ability to create and visualize a common operating picture (with augmented reality, wearables, and other intelligence).

A future area for examination is the satellite-to-device capabilities being launched to provide service from space across the U.S. where it is impossible to deploy terrestrial cell towers. This service will be available on the FirstNet network soon, and it will be important to stress test this functionality for public safety communications in remote and disaster hit areas.

Question 2. 47 U.S.C. § 1443 outlines a process for public safety wireless communications research and development. Do you believe the FirstNet Authority could strengthen its collaboration with nearby NIST and NTIA ITS labs with respect to public safety communications research? If yes, please elaborate on how this collaboration could be strengthened.

Answer. Yes. The FirstNet Authority, NTIA ITS, and NIST PSCR have a very strong partnership with multiple collaborations over the years. The labs regularly work together to ensure they are maximizing collaboration opportunities in a fiscally responsible manner.

The FirstNet Authority has more recently engaged in joint working group discussions with the NTIA-ITS Boulder lab regarding additional public safety communications opportunities and projects in the NTIA-ITS 5G CRAIN lab focused on spectrum interference.

Question 3. Would you support or oppose cuts to Federal funding to labs, including the aforementioned labs, which support the advancement of communications research?

Answer. I support continued support for all the Department of Commerce labs focused on advancing public safety communications technology, and there may be additional efficiencies in more unified collaboration.

Question 4. The Public Safety Trust Fund was only authorized until Fiscal Year 2022. From your perspective, describe how reinvestments are made into the FirstNet Authority's lab and highlight where additional Federal resources may be needed for public safety communications research.

Answer. The FirstNet Authority lab is funded by the annual FirstNet Authority Budget approved each year by the Board. The Board has made significant investments in capabilities in our FirstNet Boulder Lab since 2014. It is an important asset in the contract oversight function of the network and is continuously updated to ensure the latest public safety capabilities can be fully tested under severe congestion scenarios to ensure FirstNet public safety subscriber services work as designed.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TED CRUZ TO
SCOTT AGNEW

Question 1. Since 2015, the Commerce Department's Inspector General (IG) has issued 19 audit and evaluation reports and two investigative reports on the FirstNet Authority highlighting modifications to the network contract that "made it easier for

AT&T to achieve milestone compliance and payment,”¹ the Authority’s failure to “adequately assess contractor performance to ensure AT&T achieved” network coverage and device connections targets,² and conduct by senior leadership that “interfer[ed] with OIG’s statutory right of access and duty to keep the Secretary of Commerce and Congress informed of serious issues affecting [the] FirstNet Authority.”³ In August, the IG issued a report finding that senior FirstNet Authority officials obstructed oversight, withheld and altered documents, directed staff not to cooperate with the IG, and cultivated an internal “warlike” relationship with the oversight office, describing the IG as their “common enemy.”⁴ That same report also found retaliation against whistleblowers, including efforts to pressure at least one employee to resign, which led the IG to take the highly unusual step of making a criminal referral to the Department of Justice.

Other IG reports have raised serious questions about the Authority’s management of its contract with AT&T. In May 2024, the IG stated that the Authority “did not ensure . . . desired results for both coverage and device connection targets for each state and territory” were achieved due to the decision to “accept[] AT&T’s proposed nationwide coverage metrics” and “repeatedly chang[e] device connection target requirements from state-by-state to a less stringent nationwide basis.”⁵ Absent this, “AT&T would not have met the originally contracted state-by-state requirement for 34 states and one territory.”⁶ Follow up audits in June 2024 reinforced these findings.⁷

These reports raise questions about the Authority’s governance and its oversight of its contract with AT&T. Some have pointed to the Authority’s nebulous “independent” status in Federal statute as part of the reason for the lackluster accountability.

a. Please respond to the IG’s findings referenced above.

b. Would making the Authority directly accountable to NTIA be a positive or negative change, and why?

Answer. AT&T supports rigorous oversight of government programs such as FirstNet. FirstNet operates under arguably the strongest, most layered oversight mechanisms in Federal telecommunications. Those mechanisms are a healthy, deliberate safeguard Congress built into the program; they work as intended and continue to strengthen the network that first responders rely on every day. This ensures the network continuously evolves in direct response to public safety’s needs—a distinguishing feature that separates FirstNet from commercial, best-effort wireless networks, which aren’t subject to such reviews.

The Department of Commerce OIG maintains a dedicated team that conducts continuous audits and investigations of FirstNet. The management alerts and reports help identify opportunities to strengthen oversight, and the FirstNet Authority has used those recommendations to improve processes and controls. While the OIG’s reviews are primarily focused on internal government processes and opportunities to strengthen contract oversight, as the network contractor, AT&T has been named in some of these reports. Where the OIG issues findings related to AT&T operations and performance, it has been unfortunate that the OIG has refused direct feedback from AT&T despite multiple attempts and offers to provide information. This has, on occasion, resulted in incorrect information, a lack of context and a limited scope of AT&T activity being contained in OIG reports. AT&T welcomes the oversight from the OIG and would welcome the opportunity to be a resource to increase the accuracy and effectiveness of these reviews.

¹Department of Commerce Office of Inspector General, *FirstNet Authority Did Not Ensure the Nation’s First Responders’ Needs Were Continuing to Be Met Timely When Modifying Key Objectives of the NPSBN Contract*, OIG–24–024–A (2024), https://www.oig.doc.gov/OIGPublications/OIG-24_2.pdf.

²Department of Commerce Office of Inspector General, *FirstNet Authority’s Lack of Contract Oversight for Device Connection Targets Puts the NPSBN at Risk of Impacting First Responders’ Use of the Network*, OIG–24–027–A (2024), <https://www.oig.doc.gov/wp-content/OIGPublications/OIG-24-027-A-REDACTED.pdf>; Department of Commerce Office of Inspector General, *FirstNet Authority’s Lack of NPSBN Contract Oversight for Coverage Puts at Risk First Responders’ Ability to Serve the Public Effectively*, OIG–24–026–A (2024), <https://www.oig.doc.gov/wp-content/OIGPublications/OIG-24-026-A-REDACTED.pdf>.

³Department of Commerce Office of Inspector General, *Investigation into Allegations That FirstNet Authority Senior Officials Interfered with OIG Audits*, OIG–24–0175 (2025), https://www.oig.doc.gov/wp-content/OIGPublications/Public_Investigative_Summary_24-0175_SECURED.pdf.

⁴*Id.*

⁵*Supra* note 1.

⁶*Id.*

⁷*Supra* note 2.

As contractor, AT&T defers to government stakeholders on the best governance structure to achieve the government's goals for the FirstNet program.

Question 2. FirstNet arose out of a recommendation from the 9/11 Commission to establish a nationwide, interoperable network dedicated to public safety officials to achieve interoperability after communication failures on 9/11 meant firefighters, police officers, and other first responders couldn't talk to one another because they were using incompatible radio systems. Does FirstNet, as it exists today, adequately address the concerns raised by, and recommendations from, the 9/11 Commission Report?

Answer. Yes, FirstNet directly addresses the concerns raised by and recommendations from the 9/11 Commission Report, but as discussed below, the mission is not complete. Public safety's network is here, it's working, and it's trusted by and serving public safety in rural, urban, suburban, tribal and territorial communities. But the work is not done. The FirstNet network must continue to expand, as designed by Congress, to provide services in hard-to-reach areas as prioritized by public safety.

In addition, based on public safety's direct feedback, we are now bringing the next generation of interoperability to public safety by integrating broadband services with legacy land-mobile radio systems, which have long served public safety for push-to-talk (PTT) voice services.

As part of the successful, self-sustaining program model, significant investment has been made in FirstNet mission-critical, broadband-enabled PTT. FirstNet Fusion will take interoperability to the next level by enabling interoperability for these previously siloed LMR systems and allowing for the Fusion mobile application to operate across FirstNet and other non-FirstNet carrier devices.

For additional context, FirstNet is interoperable with commercial wireless networks based on common, international standards—a requirement set by the U.S. Congress in the 2012 enacting statute. And as America's public safety network, FirstNet delivers first responders with a dedicated network core, always-on, multi-tier priority and preemption, dedicated deployable assets for emergencies and planned events, as well as dedicated connectivity across public safety's Band 14 spectrum when and where it's needed. That means FirstNet users can call, text and exchange data (and vice versa) with other first responders regardless of wireless network. And with FirstNet Fusion, the brick wall between wireless broadband and LMR is crumbling. In short, it is no longer a technology issue, but a matter of public safety awareness, education and adoption.

Question 3. Congress authorized FirstNet in 2012, and the contract was awarded to AT&T in 2017. Since then, the communications sector has experienced massive technological advancements, including the transition from 4G LTE to 5G; the rise of satellite-based direct to cell technology; and new network management tools like network slicing and AI for dynamic management. Future developments—including 6G and dynamic spectrum sharing—are just around the corner.

a. Given modern communications technologies are built upon 3GPP standards that ensure interoperability, what is the continued need for a single nationwide network like FirstNet if the goal is to ensure interoperability?

i. Is there anything preventing first responders who today subscribe to, for example, Verizon Frontline wireless service, from texting, calling, or otherwise communicating with first responders who subscribe to T-Priority or FirstNet (other than potential differences in network coverage)? If not, then what interoperability concerns truly remain (land mobile radio notwithstanding)?

Answer. Congress and public safety envisioned a single nationwide public safety network for a reason: a single nationwide network to ensure seamless interoperability, consistent performance, high levels of security, clear accountability, and to ensure the network continues to evolve based on first responders' needs. Without a single nationwide network, like FirstNet, we risk recreating the fragmented, high-risk patchwork that failed first responders on 9/11.

Additionally, FirstNet is a catalyst for public safety-centric innovation and competition across the broader wireless ecosystem. It has established a higher standard for reliability, priority, security and resiliency—raising the bar for the entire market and therefore benefiting all first responders—regardless of whether they are FirstNet subscribers or use a commercial wireless service.

There is nothing preventing first responders who today subscribe to commercial service offerings, such as Verizon Frontline or T-Mobile's T-Priority, from texting, calling, or otherwise communicating with first responders who subscribe to FirstNet. FirstNet is interoperable with commercial wireless networks based on common, international standards—a requirement set by the U.S. Congress in the enacting statute in 2012. And as America's public safety network, FirstNet delivers first re-

sponders with a dedicated network core, always-on, multi-tier priority and preemption, dedicated deployable assets for emergencies and planned events, as well as dedicated connectivity across public safety's Band 14 spectrum when and where it's needed. That means FirstNet users can call, text and exchange data (and vice versa) with other first responders regardless of wireless network.

While there are priority offerings available to public safety from commercial, best-effort wireless service providers, public safety on those networks have reported continued challenges with network congestion during operationally critical response incidents. This was the case for public safety and other emergency response personnel during the presidential assassination attempt at the campaign rally in Butler, PA. Despite widespread accounts of network congestion on wireless networks, the U.S. House Butler Task Force found "law enforcement personnel with FirstNet cellular service did not have notable interference with their connectivity."⁸

As part of the successful, self-sustaining program model, significant investment has been made in FirstNet mission-critical, broadband-enabled PTT—bringing the next generation of interoperability to public safety. FirstNet Fusion will take interoperability to the next level by enabling interoperability for previously siloed land-mobile radio (LMR) systems and allowing for the Fusion mobile application to operate across FirstNet and devices on commercial networks. This work reflects the FirstNet public-private partnership's commitment to continuous improvement, future readiness, and responsiveness to first-responder's feedback and evolving needs.

Question 4. Many public safety officials subscribe to multiple services, in addition to FirstNet, to achieve redundancy or coverage where FirstNet may be lacking. As part of a reauthorization effort, does Congress need to act to preserve this redundancy in the marketplace or will it exist sans legislative action?

Answer. Redundancy in the marketplace exists today and will continue without direct legislative action as part of reauthorizing the FirstNet Authority. This is in part due to FirstNet acting as a catalyst for public safety-centric innovation and competition across the broader wireless ecosystem. FirstNet instead establishes a higher standard for reliability, priority, security and resiliency—raising the bar for the entire market and therefore benefiting all first responders—regardless of whether they are FirstNet subscribers or use a commercial wireless service.

Commercial offerings like Verizon Frontline and T-Mobile's T-Priority—which did not exist prior to FirstNet—may claim comparable capabilities, but only FirstNet delivers a purpose-built network for public safety with a dedicated network core, dedicated deployable assets, multi-tier priority and preemption, a mandate to never throttle public safety's critical communications, and rigorous Federal accountability. This provides public safety with heightened performance and functionality that is superior to commercial, best-effort service offerings.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN THUNE TO
SCOTT AGNEW

Question 1. Rural states, like South Dakota, rely crucially on the coordination between federal, state, tribal, and local governments to respond to emergencies. How has AT&T navigated coordination at the national level across all 50 states and territories with relevant Federal agencies, such as the U.S. Department of Defense, U.S. Department of Justice, and U.S. Department of Homeland Security, to ensure robust public safety?

Answer. From the outset, FirstNet was built for, and informed by, public safety. This is why our FirstNet Response Operations Group (ROG) is led by a dedicated team of former first responders available 24x7x365 to support public safety's emergency communications needs. FirstNet ROG functions under the U.S. Department of Homeland Security's Incident Command System (ICS) principles—a standardized, on-scene management framework to effectively organize and coordinate emergency response to incidents of any size or type. This system ensures that, regardless of discipline or geography, federal, state, tribal and local agencies operate with a common operating model, shared terminology, and clear roles and responsibilities. FirstNet ROG Division Chiefs are organized by the 10 FEMA regions—which includes all states and U.S. territories. Additionally, the FirstNet ROG team includes a Federal Division Chief with a law enforcement background, allowing an understanding of Federal public safety's emergency communications needs, especially law enforcement agencies like DEA, FBI, ATF, DOJ and DHS.

⁸ <https://taskforce.house.gov/sites/evo-subsites/july13taskforce.house.gov/files/evo-media-document/12-5-2024-Final-Report-Redacted.pdf> (Page 96)

This structure and unprecedented engagement with public safety is exemplified at the annual Sturgis Motorcycle Rally in Sturgis, SD. In anticipation of large crowds at the rally each year, FirstNet ROG engages with federal, state and local law enforcement agencies to plan and identify critical communications needs months in advance. Throughout the weeks-long event, the team monitors the FirstNet network and has portable cell sites and other communications solutions at the ready to deploy as needed based on public safety's needs.

Our public-private partnership with the FirstNet Authority drives unique relationships and ability for joint government-to-government engagement. To further support the unique needs of each state, we encourage public safety entities such as South Dakota Emergency Management Agency (EMA) to participate in the process of developing a State Engagement Program Profile with FirstNet ROG and the FirstNet Authority. Our State Engagement Program builds upon our already robust response process and identifies state-specific requirements and procedures to support state emergency operation activations and develops a written playbook for enhanced operations and effective joint coordination.

Question 2. Follow-up: How can AT&T improve coordination with Federal agencies to determine and mitigate vulnerabilities to FirstNet infrastructure?

Answer. AT&T recognizes the critical importance of proactively identifying and mitigating vulnerabilities to FirstNet infrastructure and is steadfast in its commitment to strengthening coordination with Federal partners to further the resilience of America's public safety network. As part of this work, we continue to enhance our collaboration with agencies such as DHS, DOJ, FBI, CISA and other Federal stakeholders that maintain threat intelligence, physical security, and critical infrastructure protection responsibilities.

As designed by Congress, the FirstNet Authority Board includes designated member seats for DHS and DOJ, bringing heightened expertise and understanding of the statutory responsibility for critical infrastructure protection, cybersecurity, national incident response, and law enforcement oversight directly into the network's governance.

Our close collaboration with Federal cybersecurity organizations helps strengthen both AT&T's and the Federal government's ability to defend against evolving cyber threats and protect nationwide communications infrastructure. We participate in several information-sharing programs with Federal agencies, including with DHS/CISA through the National Coordination Center (NCC) and the Communications Information Sharing and Analysis Center (Comms-ISAC), the Joint Cyber Defense Collaborative (JCDC) and the Cybersecurity Collaboration Center at the NSA to receive alerts and guidance on emerging cyber threats, help develop coordinated defense strategies to protect critical communications infrastructure, and participate in simulation exercises to test and enhance collective incident response. In addition, FirstNet is the only network with a Security Operations Center solely dedicated to monitoring public safety's traffic 24x7x365, enabling us to more quickly respond to security threats without sacrificing usability or impacting public safety's missions.

From a physical infrastructure standpoint, copper theft is an emerging threat vector that has become a serious, nationwide problem with significant impacts on public safety and communications infrastructure. While we actively work with local law enforcement as they investigate to find those responsible, we support legislation to increase the penalties on related copper-theft crimes given the severity of impact to communications infrastructure. We will continue to work with Federal and state partners to better educate the general public and mitigate this growing threat to public safety, national security and the general public.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DAN SULLIVAN TO
SCOTT AGNEW

Operational Readiness and Maintenance:

AT&T and FirstNet Response Operations Group have responded effectively to disasters in Alaska, including undersea cable cuts and severe weather events, but Maui revealed gaps in equipment readiness.

Question 1. What specific processes does AT&T use to ensure deployable assets are continuously updated, tested, and ready to deploy without requiring emergency fixes during a disaster?

Answer. The FirstNet Response Operations Group (ROG)—led by a dedicated team of former first responders—works around the clock 24x7x365 and is responsible for managing the deployment of the dedicated FirstNet fleet. We perform established, repeatable processes designed to ensure the ongoing readiness and reli-

ability of critical disaster recovery assets. These processes include regular inspection, testing, and preventative maintenance of all FirstNet deployable assets on a monthly, quarterly, semi-annual and annual basis. In addition, we perform trip maintenance prior to and following each deployment, spanning vehicle, safety and technology-based inspections. In addition to routine mechanical and electrical system validation, the emergency communications platforms are subject to regular software updates, firmware maintenance, and licensing compliance activities throughout the year. Collectively, these measures are intended to support sustained operational capability, security, and interoperability during disaster response and public safety support operations.

FirstNet ROG has provided critical support for public safety on FirstNet in Alaska, deploying FirstNet assets in response to wildfires, the undersea cable cut impacting towns like towns like Utqiagvik (f.k.a. Barrow), Wainwright and Point Hope in the North Slope Borough; planned events, such as the Arctic Winter Games in Palmer; and was at the ready to support public safety after flooding from the remnants of Typhoon Halong. FirstNet ROG has also deployed these assets on numerous occasions to public safety training and exercises.

FirstNet is the only network with deployable assets dedicated exclusively to public safety—the direct product of requirements established by public safety and state leaders. This includes 190+ portable cell sites strategically stationed at 70+ locations across the United States. Recently, we doubled down on dedicated public safety support in Alaska, expanding the in-state FirstNet assets to include 3 FirstNet SatCOLTs (Satellite Cell on Light Trucks) and 3 new mini Compact Rapid Deployables (miniCRDs). Beyond serving as public safety's network partner, AT&T leads the way in disaster and emergency response—from investing more than \$1 billion into the industry's largest disaster recovery program since 1992 to driving cutting-edge connectivity solutions and maintaining a commercial fleet of 750+ AT&T assets.

Logistics Planning:

The OIG found that the absence of prearranged logistics agreements delayed deployment in Maui. Alaska's weather and transportation constraints make advance logistics planning even more critical.

Question 2. What logistics exercises has AT&T conducted to prove that deployable assets can be moved and activated quickly in remote areas like rural Alaska?

Answer. As public safety's partner, we welcome the opportunity to collaborate with state and local stakeholders to plan for and strengthen our coordination during disasters and other emergencies. The FirstNet Response Operations Group (ROG)—led by a dedicated team of former first responders—works around the clock 24x7x365 and is responsible for managing the deployment of the dedicated FirstNet fleet. The team is organized by FEMA Region with a FirstNet ROG Division Chief assigned to each FEMA Region.

The Division Chief for FEMA Region 10, which includes Alaska, recently spent nearly a week in Anchorage training local AT&T personnel and members of the local FBI field office on the set up and deployment of FirstNet assets—SatCOLTs (Satellite Cell on Light Trucks) and mini Compact Rapid Deployables (MiniCRDs)—in the state. Additionally, FirstNet ROG participates in the Alaska Partnership for Infrastructure Protection (APIP), which sits within the all-hazard resiliency planning unit of the State of Alaska Division of Homeland Security and Emergency Management. As part of our work with APIP, we host the APIP monthly meetings at the AT&T office in Anchorage, and recently conducted capability training with FirstNet assets, as well as state-owned Compact Rapid Deployables. As part of this exercise, teams used the FirstNet miniCRD on an offroad all-terrain vehicle and a snowcat. Overall, we find it extremely valuable to participate in trainings, exercises, and in pre-event and mutual aid planning sessions. We see training during “Blue Sky Days” as an important best practice. It improves the process for effective collaboration during emergency incidents and ensures those who will be activated to support emergency response have hands-on training and experience with the equipment before an emergency event.

Informed by our experience supporting Alaska public safety and other hard-to-reach regions of the country, we developed smaller and more portable equipment for the deployment of portable cell sites to serve first responders. MiniCRDs are the size of two suitcases and can be flown, transported by car, or carried into an incident. And because Alaska's terrain is rugged and remote, and not easily accessed by road, flying is often the fastest way to access remote areas. AT&T maintains two aircraft in Anchorage and can charter planes when needed, to deploy employees and assets to remote parts of the state. In addition, the FirstNet team also routinely collaborates with local public safety agencies to transport assets onto their aircraft to

support public safety's emergency response. A recent example includes collaboration with a local agency that transported FirstNet equipment on a local medivac jet.

Following the ice sheet that severed undersea fiber to the North Slope, FirstNet was the first to arrive to restore communications for local public safety with a miniCRD. The miniCRD had the range to offer coverage to most of the town of Utqiagvik, formerly known as Barrow. In addition to providing the only deployable asset fleet exclusively available to public safety, we were the first provider to enable agencies to own and deploy their own deployable network assets, giving them better command and control of their network. The State of Alaska has invested in their own FirstNet deployable asset, which they can directly deploy and operate during planned and emergency events.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. ERIC SCHMITT TO
SCOTT AGNEW

Question 1. AT&T holds a strong responsibility to safeguard a national public-safety network in FirstNet, with its workforce being essential to this task. In order to understand how AT&T manages this risk, what specific documents or verification steps does AT&T require its vendors to provide to confirm that every worker on its tower sites is legally authorized to work in the United States?

Answer. AT&T is committed to ensuring that our company complies with all applicable laws and utilizes a workforce legally authorized to work in the United States. As our vendors are a key part of our business and an integral part of our approach to corporate responsibility, AT&T contractually requires its primary contractors to comply with all laws and regulations applicable to them and their subcontractors' performance as well as adhere to our AT&T Principles of Conduct for Suppliers (<https://attsuppliers.com/misc/SupplierSustainabilityPrinciples.pdf>).

AT&T also contractually obligates its primary contractors and their subcontractors to use employees for its tower work and limits their use of independent contractors (IRS Form 1099 workers) to short-term services lasting less than 90 days in a calendar year and consistent with applicable laws. To enforce compliance with these requirements, AT&T recently required that its primary contractors confirm for all individuals who work on AT&T equipment that (1) their identities have been verified via their social security and drivers' license numbers; (2) their legal right to work in the United States has been verified; and (3) that no independent contractors have been engaged for more than 90 days in the calendar year. AT&T will require its primary contractors to use audited I-9 compliance to verify the legitimacy of their workforce.

AT&T has established a hotline for reports of suspected use of undocumented workers or unregistered contractors on AT&T's tower projects. We are committed to investigating such reports and taking appropriate action based on their findings.

Question 2. How frequently does AT&T conduct compliance reviews or audits to ensure that unauthorized workers are not being used on FirstNet infrastructure projects?

Answer. AT&T employs a multi-layered compliance and oversight program to help ensure that only authorized workers perform work on FirstNet infrastructure. While the frequency of reviews varies based on project activity and risk indicators, AT&T conducts regular compliance checks and audits, supplemented by continuous monitoring mechanisms designed to identify potential issues in real time. Overall, compliance oversight is not tied to a fixed calendar interval; instead, it is conducted regularly and in response to operational needs, risk factors, or specific indicators, ensuring that AT&T can swiftly address any potential concerns about unauthorized workers on FirstNet projects.

We also monitor the use of company-issued devices through security controls designed to identify potentially anomalous activity that could indicate unauthorized access or misuse, consistent with applicable law and company policy.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARIA CANTWELL TO
SCOTT AGNEW

Salt Typhoon Impact. Last June, I wrote to AT&T's CEO requesting information to understand how the unprecedented Salt Typhoon attack impacted not only AT&T's commercial network but also whether the FirstNet network was affected as well.

I asked for the third-party threat assessments that would supposedly verify their claim that their networks were now secure from the next Chinese cyber attack. But AT&T has chosen not to cooperate.

I made the same request of Verizon and also didn't receive anything.

In the face of increasingly sophisticated attacks like the Chinese state-sponsored Salt Typhoon, public safety users should have confidence that the network they are using is secure and protected.

Question 1. Did the Salt Typhoon attacks penetrate the FirstNet network, yes or no?

Answer. All major U.S. telecommunications carriers, including AT&T, were victims of the Chinese state-sponsored hackers known as "Salt Typhoon." This was an unprecedented attack that was carried out by an incredibly sophisticated state actor, who also penetrated U.S. government systems.

Question 2. If no, is there a third-party assessment that confirms this? If so, do you commit to giving me that document?

Answer. N/A

Question 3. If the Salt Typhoon attackers did penetrate the FirstNet network, is there a third-party assessment confirming they have been fully evicted? If so, do you commit to giving me that document?

Answer. AT&T retained Mandiant, a leading third-party cyber defense specialist to assist our own network and cybersecurity experts with our investigation. Together, we conducted digital threat surveillance, threat hunting, digital forensics, and in-depth attack analysis to locate and monitor the intrusion points and triage as necessary. In March 2025, Mandiant verified that AT&T had contained the cyber incident brought on by this threat actor and we have not identified evidence of Salt Typhoon activity inside the AT&T network since October 7, 2024.

Question 4. Has Mandiant or another third-party identified any network vulnerabilities, on FirstNet or otherwise, exploited by Salt Typhoon attackers that AT&T has not fully remediated, yes or no?

Answer. Cybersecurity is one of the biggest challenges facing the connected world. With the rise of ever-more sophisticated threats and nation-state actors and accessible hacking technologies, attacks are growing in both volume and complexity. To protect businesses and customers, organizations must adopt a robust proactive approach to identifying and mitigating cyberattack risks.

We defend the AT&T & the FirstNet networks with a multi-layered approach, including monitoring, active prevention and rapid response to security threats. We leverage tools, where available, that include near-real-time data correlation, situational awareness reporting, active incident investigation, case management, trend analysis and predictive security alerting.

We assess, identify and manage risks from cybersecurity threats through various mechanisms. We conduct vulnerability testing and assess identified vulnerabilities for severity, the potential impact to AT&T and our customers, and likelihood of occurrence. Our security teams work with applications and system owners to remediate those vulnerabilities.

In sum, network security requires a multifaceted approach to stay ahead of malicious actors. AT&T continues to harden its network and configurations to further safeguard our network against future incidents.

Question 5. Has Mandiant or another third-party made any security recommendations that AT&T has not fully implemented in the FirstNet network, yes or no? This includes, but is not limited to, patching network edge devices such as VPNs, firewalls, and routers, and implementing phishing-resistant multi-factor authentication.

Answer. See Answer to Question 4 above.

Outstanding GAO and OIG Recommendations. The Government Accountability Office and the Department of Commerce's Inspector General released a number of extremely troubling reports that have raised serious concerns about a troubling pattern: when AT&T falls short of its contractual requirements, the response has been to change how performance is measured rather than to actually improve performance.

When AT&T failed to meet FirstNet adoption requirements in 34 states, the Authority replaced strict state-by-state standards with a nationwide average—a change AT&T itself proposed—allowing \$38 million in penalties to be waived. When AT&T was on track to miss deployment targets in rural communities, the Authority changed how deployment was calculated, helping AT&T avoid penalties and collect additional payments.

And with the Maui wildfires, the OIG found that AT&T altered data after the fact. AT&T downgraded requests for temporary cell sites from requiring immediate

action to a lower priority. The report documented staff comments about “backdating” request times and needing to “pad my stats.” The FirstNet Authority failed to catch this until the Inspector General brought it to their attention.

Mr. Agnew, will you commit that AT&T will not alter data or provide inaccurate information to the FirstNet Authority, and that AT&T will stop seeking contract modifications designed to weaken performance standards?

Answer. AT&T is committed to performing its responsibilities as the FirstNet contractor with the highest level of integrity. AT&T has not and will not seek contract modifications that weaken performance standards for the network.

As the network contractor, AT&T welcomes the rigorous oversight and accountability that is applied to the FirstNet program. FirstNet operates under extraordinary oversight—arguably the strongest, most layered oversight mechanisms in Federal telecommunications. Those mechanisms are a healthy, deliberate safeguard Congress built into the program; working as intended and continue to strengthen the network that first responders rely on every day. This ensures the network continuously evolves in direct response to public safety’s needs—a distinguishing feature that separates FirstNet from commercial, best-effort wireless networks, which aren’t subject to such reviews.

Regarding the two reports referenced in this question, I’m happy to provide additional clarity on these issues.

The original FirstNet build and adoption plan, developed in 2017, included annual progress projections and assumptions. On an aggregate basis, AT&T exceeded those projections. In accordance with Federal Acquisition Regulation (FAR)-based contract standards, as real-world conditions evolved, the FirstNet Authority allowed limited adjustments in select states, but only in exchange for AT&T accepting more aggressive adoption and coverage requirements at a state and national level than was originally required for delivery.

Unfortunately, the OIG did not include in its report that the Federal government received clear, quantifiable concessions in exchange for the contract modification. The contract modification didn’t represent leniency or a weakening of performance; instead, it delivered real value to the government and public safety, including:

- Delivering more sites than originally required, expanding public safety’s Band 14 spectrum coverage in rural areas and reaching several hundred thousand additional square miles beyond our target commitment.
- Exceeding original nationwide adoption targets, achieving the nationwide total nearly 8 months in advance.

Second, regarding the OIG’s audit report on the Maui wildfires, I again want to be clear that AT&T welcomes the constructive feedback from the OIG, which leads to continuous program improvements. We do, however, have deep concerns with several inaccuracies and an incomplete account of the FirstNet response, as presented in the OIG’s report, which has led to factual inaccuracies and unwarranted conclusions. AT&T submitted a formal response that is available on the OIG’s website: https://www.oig.doc.gov/wp-content/OIGPublications/OIG-25-004-A-NGO_Response.pdf.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. BRIAN SCHATZ TO
SCOTT AGNEW

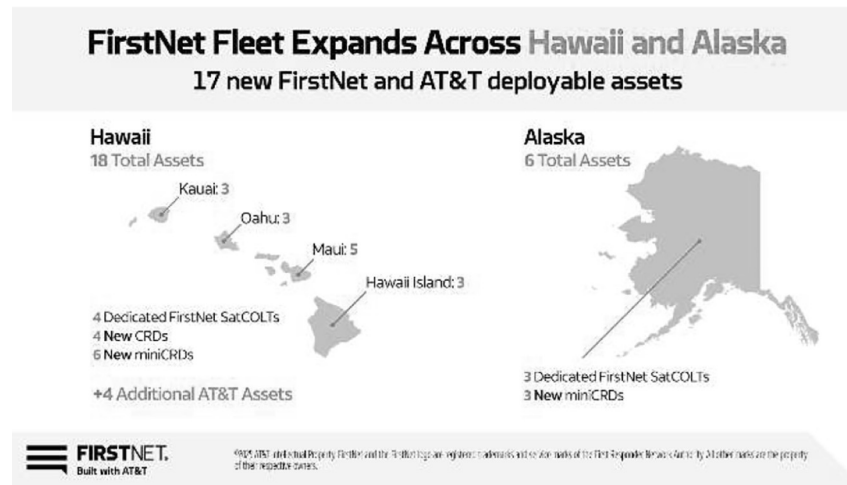
Question 1. In December 2024, the Department of Commerce Office of Inspector General issued a report, “Nationwide Public Safety Broadband Network Was Not Always Available to First Responders During the Catastrophic 2023 Maui Wildfires.” What is the status of AT&T’s compliance with, and implementation of, the eleven recommendations from the report?

- a. What is the status of any pending recommendations?
- b. When can you guarantee these recommendations will be fully implemented?

Answer. The Department of Commerce’s Office of Inspector General’s audit, report, and recommendations were directed to the FirstNet Authority. AT&T, as the contractor, has supported the FirstNet Authority’s efforts to address the recommendations. Based on information provided by the FirstNet Authority, all 11 recommendations have approved action plans. Nine recommendations have been implemented and the remaining 2 are in progress.

Above and beyond AT&T’s formal contractual obligations to the FirstNet Authority, AT&T recently made a significant investment to expand deployable network assets across the islands of Hawaii and in Alaska. We are committed to learning from each major response event, and we continuously apply these learnings to improve

our readiness and operations to support public safety. In December 2025, we joined fire service leaders from across Hawaii at the Hawaii Fire Chiefs annual conference to announce the significant AT&T investment in Hawaii that adds 10 FirstNet assets, as well as 4 AT&T deployable assets across Hawaii. For Maui specifically, we incorporated feedback from the Maui Fire Chief as we designed this plan to expand the on-island FirstNet deployable assets available in Hawaii. Based on his feedback, we added assets to the smaller Maui County islands of Moloka'i and Lana'i. The graphic below provides a visual representation of the FirstNet and AT&T deployable assets that are now available across Hawaii and Alaska. More information is available here: <https://about.att.com/blogs/2025/ready-for-anything.html>.



Question 2. Why did AT&T include Hawaii in its business continuity and disaster recovery plan for the continental United States?

- What oversight and approval protocol was in place at the time of AT&T's development and approval of the plan? What specific gaps contributed to this error?
- What changes have been made at AT&T to address these oversight and approval errors?
- What protocols are now in place to ensure that AT&T's plan for Hawaii reflects the very real needs of the state during an emergency?
- Did AT&T work with Hawaii state public safety officials in the development and approval of the previous business continuity and disaster plan?
- Will AT&T now work with Hawaii state public safety officials in the development and approval of the new business continuity and disaster plan?

Answer. Every year, AT&T submits its Business Continuity and Disaster Recovery (BCDR) plan to the FirstNet Authority for review and acceptance. The BCDR plan had been inclusive of a nationwide response and detailed how business continuity and disaster recovery should be performed. These plans are continuously refined based on lessons learned from real-world events, including the 2023 Maui wildfires.

Following the OIG's review related to the Maui wildfires, the FirstNet Authority rescinded approval of AT&T's previously submitted and approved BCDR plan. AT&T worked to further refine the plan, including adding language related to network hardening in specific geographic areas. This revised plan was resubmitted by AT&T and accepted by the FirstNet Authority.

AT&T also worked with state and local public safety stakeholders in Hawaii to identify priority areas, which informed AT&T's resiliency efforts in Hawaii.

I have previously directed an internal taskforce to further customize and refine the BCDR plan for Hawaii, given the unique needs and requirements presented during emergency response. I would gladly keep your office updated on these efforts as we continue our commitment to continuously strengthen our operations and preparedness in Hawaii. I had the opportunity to meet with first responders in Hawaii following the Maui wildfires and understand the criticality of reliable, dedicated communication to support their response to operationally critical incidents. Ensuring

ing Hawaii has robust access to FirstNet support and reliable network performance is a top priority for me. As we continue acting on lessons learned and implement improvements to strengthen our response readiness, we will continue to work with public safety stakeholders in Hawaii to ensure their feedback informs our efforts.

Question 3. The first recommendation from the Office of the Inspector General report directs FirstNet to ensure that special hardening measures are implemented for the unique threats faced in the Maui region, as required by the NPSBN contract. What specific hardening measures have been taken to address this recommendation?

a. What other hardening and resiliency measures have been taken aside from deployables?

b. Have additional hardening measures been adopted for other high-risk areas since the Office of the Inspector General report was released?

c. Are additional hardening measures, aside from deployables, planned for other high-risk areas?

Answer. Following any major event, AT&T evaluates our response and network performance and looks for opportunities to improve and strengthen the network and response operations.

AT&T made significant investments to increase the hardening of assets in Hawaii after the Maui wildfires. These investments include the addition of 4 portable generators that are stored locally on Maui; we have repaired and/or rebuilt all damaged and destroyed towers on Maui; and we have also launched 3 new cell towers on Maui, to further expand wireless coverage and capacity. AT&T is warehousing additional inventory of spare equipment and parts, locally on Maui, to support more rapid restoration of services and hardware when the need arises.

In addition, AT&T has contracted with an on-island vendor to provide additional surge capabilities for additional generators, if needed, during response activities. AT&T now has dedicated on-island technical personnel who can respond more immediately when incidents occur, instead of needing to arrange transport for personnel from the other Hawaiian Islands to Maui. Other technical resources can be deployed from other islands when needed. Just as AT&T does with any major response, we can surge additional personnel and assets to an impacted area, but now with these new on-island Maui investments, we have personnel and additional equipment in the county to support immediate response activities while AT&T simultaneously surges additional response resources as needed.

Beyond hardening, AT&T is also engaged with state and local public safety agencies in Hawaii to strengthen coordination during emergency response. The FirstNet program at AT&T has increased its proactive outreach to customers during network-impacting events and additional enhancements have been made to FirstNet Central, the network status tool that provides an unparalleled level of visibility to public safety on network status and outage alerting. Customer feedback indicates that FirstNet communications and network visibility exceeds what they experience from commercial, best-effort service offerings.

To further support the unique needs of each state, we encourage public safety entities to participate in the process of developing its State Engagement Program Profile (playbook) with our FirstNet Response Operations Group (ROG). FirstNet ROG is led by a dedicated team of former first responders available 24x7x365 to support public safety's emergency communications needs. Our State Engagement Program builds upon our already robust response process by identifying state-specific requirements and procedures and developing a written playbook for enhanced operations. AT&T offered to support the development of an emergency management playbook between FirstNet ROG and the State of Hawaii.

AT&T has also requested coordination with Hawaii emergency services agencies in charge of inter-island barge transportation to provide recognition and prioritization of FirstNet assets on inter-island transport. During the May 2025 Statewide Communication Interoperability Program (SCIP) meeting, AT&T met with public safety and transit stakeholders to evaluate rapid transportation options for network assets during emergencies. AT&T is continuing to build upon these discussions and would like to formalize a proactive plan for increased rapid transport options in the future.

Finally, the FirstNet network core is being upgraded to 5G stand-alone across the country, including in Hawaii, and we are harnessing low earth orbit (LEO) satellite connectivity for the FirstNet deployable fleet. We are also excited about the enhanced reliability and redundancy that will come through satellite-to-device connectivity to extend the reach of connectivity and restore connectivity during times of network disruption, such as in hurricane and wildfire response scenarios.

I welcome the opportunity to keep you and your congressional staff updated on these network activities.

Question 4. The Office of the Inspector General report found that AT&T altered data it reported to FirstNet Authority regarding the Maui wildfire response, and that FirstNet Authority did not have access to AT&T's real time network data. Why did AT&T alter this data?

a. According to the report, AT&T downgraded first responders' requests for 14 deployables from "emergent" (requiring immediate action) to "urgent" (requiring action between 14 hours and 30 days). Why were these requests reclassified from "emergent" to "urgent"?

b. What are the standards for reclassifying first responder requests?

c. How frequently does FirstNet reclassify first responder requests?

d. What was the effect of reclassifying these requests from "emergent" to "urgent" on Maui wildfire response efforts?

e. According to the report, a deployable was inaccurately reported as meeting the 14-hour requirement. Why was the deployable inaccurately reported as meeting the requirement?

f. How is AT&T implementing new protocols to ensure that these errors do not happen again, and that data-sharing with FirstNet Authority is transparent, accurate, and trustworthy?

Answer. Following the concerns raised by the OIG, the FirstNet Authority and AT&T performed a subsequent review of the submitted compliance report and determined the actual data submitted in the compliance report was correct. For context, a request status can be reclassified based on two main factors: a) if the customer changes their request timing or b) if, during the entry of the request, an incorrect time is entered, and the correct time changes the urgency, the request is reclassified. For example, if public safety knows they will be moving a mobile command post and wants to notify us of the future location, the request would be reclassified from emergent to urgent because they want the solution delivered at a later time than actually requested.

To be clear, during the Maui response, no requests were reclassified due to an inability to meet customer-requested timing.

In addition, AT&T implemented the following process changes based on the OIG's feedback on the Maui wildfires:

- Capturing the justification for reclassifications for all requests.
- Implementing a new standard procedure for capturing the times to fulfill requests when ROG team members are in the field to support public safety and actively deploying solutions at public safety's request. The new process avoids the need for manual validation (through internal audit) during a post-event review.
- Working with the FirstNet Authority to modify the contract to simplify and clarify deployment type definitions and quality metric calculations.

AT&T welcomes the constructive feedback from the OIG, which leads to continuous program improvements, and appreciates the OIG raising these concerns, so subsequent review and validation could be performed by AT&T and the FirstNet Authority. Unfortunately, the OIG's Final Report does not make clear that AT&T and the FirstNet Authority completed the subsequent review and ultimately confirmed the calculated response time data were accurate.

Question 5. During the Maui wildfire response, why did AT&T deny first responders' initial request to deploy the SatCOW already positioned on Maui?

Answer. AT&T has no record, documentation, or knowledge of any deployable request on August 8. The first documented request came on August 10, and the on-island FirstNet deployable was delivered that same day. We formally raised this error with the OIG, but it was not corrected in the final report.

Question 6. During the Maui wildfire response, why did AT&T prematurely remove the SatCOW providing coverage to the Maui Sheraton Hotel?

Answer. Thank you for the opportunity to correct this narrative. This characterization is inaccurate.

The FirstNet SatCOW referenced in this question remained on site to support public safety while the network stabilized. It was later demobilized only after the macro network was restored and the assets had been off-air for several days.

August is Hawaii's hurricane season, and there were active wildfire risks across other islands, so returning assets to staging was essential to ensure readiness for the next emergency. Following demobilization of assets, public safety on FirstNet

has the ability to submit subsequent requests for deployable support. Upon learning of in-building connectivity challenges at the Maui Sheraton Hotel, the FirstNet Response Operations Group (ROG) installed an in-building connectivity solution to extend the restored outdoor coverage from the macro network within the building.

In a meeting with public safety officials in Hawaii, they told us they wanted more communication around demobilization decisions. We agreed and have incorporated that feedback into improved best practices moving forward.

Question 7. The Office of the Inspector General report found that FirstNet Authority did not ensure that AT&T's After-Action Report for the Maui wildfires included sufficient information about lessons learned and process and protocol improvements to implement. This is a requirement of the NPSBN contract. Why did AT&T not include this information in the report?

Answer. Per the contract, the FirstNet Authority can request after-action review following emergency events or other incidents. Following the Maui wildfires, the FirstNet Authority directed AT&T to prepare an After-Action Report. AT&T submitted the report and had subsequent meetings with the FirstNet Authority to review, answer questions, and act on lessons learned. All questions raised by the FirstNet Authority were addressed through the After-Action Report process, which was formally accepted by the FirstNet Authority in Oct. 2023.

Question 8. How are deployables tested and assessed for readiness, and what training and resources are offered to state and local public safety officials?

a. What is the frequency of the training provided to state and local public safety officials?

Answer. The FirstNet Response Operations Group (ROG)—led by a dedicated team of former first responders—works around the clock 24x7x365 and is responsible for managing the deployment of the dedicated FirstNet fleet. We perform established, repeatable processes designed to ensure the ongoing readiness and reliability of critical disaster recovery assets. These processes include regular inspection, testing, and preventative maintenance of all FirstNet deployable assets on a monthly, quarterly, semi-annual and annual basis. In addition, we perform trip maintenance prior to and following each deployment, spanning vehicle, safety and technology-based inspections. In addition to routine mechanical and electrical system validation, the emergency communications platforms are subject to regular software updates, firmware maintenance, and licensing compliance activities throughout the year. Collectively, these measures are intended to support sustained operational capability, security, and interoperability during disaster response and public safety support operations.

Public safety agencies on FirstNet have access to a dedicated fleet of deployable assets that are available free of charge and can be requested to support planned and emergency event response, including federal, state and local training events. Public safety can request deployable support through a variety of ways, including the FirstNet Central network status tool, calling a 1-800 phone number, or submitting a request through their account representative. Educating public safety about the request process is part of customer onboarding. Additionally, the FirstNet Response Operations Group (ROG) is organized by the 10 FEMA regions, and the incident command lead for each region is available to participate in emergency trainings and exercises. This allows public safety to learn about and practice how they can request these resources.

Question 9. How does FirstNet determine its metrics for deployment success?

Answer. The metrics for the deployment of deployable assets are included in the AT&T/FirstNet Authority contract, which includes a nationwide 14-hour response time objective for fulfillment of emergency deployment requests. As the FirstNet contractor, AT&T has assets staged in more than 70 locations across the country to support the timely delivery of FirstNet dedicated deployable assets. AT&T regularly responds well in advance of this 14-hour objective.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN HICKENLOOPER TO
SCOTT AGNEW

Federal Labs. Colorado is home to many Federal labs which perform mission critical research, development, and testing to improve communications service. The First Responder Network Authority, the NTIA's Institute for Telecommunications Sciences (ITS), and NIST's Public Safety Communications Research Division within the Communications Technology Laboratory all call Boulder, Colorado their home. The FirstNet Authority's lab in Boulder tests public safety technologies which will be used by first responders. NTIA's ITS lab is the gold standard for researching how

to maximize spectrum efficiency and reduce interference to Federal agency missions and commercial radiofrequency applications. NIST's PSCR Division supports the development of technical specifications to advance next-generation communications technologies.

Question 1. Do you believe the research activities performed by the NIST, NTIA, and FirstNet Authority Labs are key to the success of advancing the state of the art in public safety communications? Which areas of research or technical challenges in public safety communications may be useful to examine going forward?

Answer. The research performed by the National Institute of Standards and Technology (NIST), the National Telecommunications and Information Administration (NTIA), and the First Responder Network Authority (FirstNet Authority) Labs is essential to advancing public safety communications. These organizations provide a rigorous, science-driven foundation that allows industry and government to independently validate emerging technologies before they are deployed at scale. In addition to formal research, these labs offer a unique demonstration and testing environment where public safety agencies, policymakers, and industry partners can observe capabilities, concepts, and performance in realistic operational scenarios that don't come at the expense of reliability or interoperability, which is crucial in mission-critical environments. This collaborative ecosystem accelerates the translation of research into deployable, trusted solutions for first responders.

Looking ahead, research and lab testing will be essential for innovative public safety-centric solutions, including but not limited to AI-enabled capabilities, device form factors focused on the connected responder via IoT, and off-network and device-to-device communications that operate across multiply communication types. For example, public safety operations routinely transition between in-coverage, out-of-coverage, and degraded conditions, often within a single incident. Evaluating how devices can dynamically support direct communications—using broadband, legacy systems such as LMR, or hybrid approaches—helps ensure first responders remain connected when infrastructure is unavailable or stressed.

Question 2. 47 U.S.C. § 1443 outlines a process for public safety wireless communications research and development. Do you believe the FirstNet Authority could strengthen its collaboration with nearby NIST and NTIA ITS labs with respect to public safety communications research? If yes, please elaborate on how this collaboration could be strengthened.

Answer. Overall, the existing partnership among the FirstNet Authority, NIST and NTIA ITS labs is strong and performs well for the public safety communications ecosystem. Continued coordination and integration will help ensure Federal research investments translate into trusted, tested solutions that meet the evolving needs of first responders. Today, these organizations work in complementary ways to help ensure that research priorities remain grounded in operational reality and that new technologies are evaluated before being introduced into mission-critical environments. By increasing operational feedback loops between laboratory research and field deployments, this collaboration could be further strengthened and, ultimately, better inform research priorities to benefit public safety.

Question 3. Would you support or oppose cuts to Federal funding to labs, including the aforementioned labs, which support the advancement of communications research?

Answer. Federal research labs such as NIST, NTIA ITS and the FirstNet Authority lab play a critical role in advancing the science, standards, and testing need, which supports secure, resilient and interoperable communications—particularly for mission-critical public safety use cases. The FirstNet program, which includes the FirstNet Lab in Boulder, Colorado, is designed to be self-sustaining and does not rely on Federal appropriations for its ongoing operations. The FirstNet Authority reinvests program revenues back into the network and related activities (such as the FirstNet Lab) to continuously improve public safety communications capabilities. This model allows the FirstNet Authority to support innovation and operational enhancements—all based on public safety's needs and direct feedback. Continued Federal investment in NIST and NTIA ITS ensures a strong, independent research foundation that benefits the broader communications ecosystem, including public safety.

Question 4. The Public Safety Trust Fund was only authorized until Fiscal Year 2022. From your perspective, describe how reinvestments are made into the FirstNet Authority's lab and highlight where additional Federal resources may be needed for public safety communications research.

Answer. The FirstNet program, which includes the FirstNet Lab in Boulder, Colorado, is designed to be self-sustaining and does not rely on Federal appropriations for its ongoing operations. As required by the enacting statute of the FirstNet pro-

gram and the FirstNet/AT&T contract. AT&T pays the FirstNet Authority sustainability payments for the use of Band 14 spectrum. In turn, the FirstNet Authority reinvests these program revenues back into the network and related activities (such as the FirstNet Lab) to continuously improve public safety communications capabilities. This model allows the FirstNet Authority to support innovation and operational enhancements—all based on public safety’s needs and direct feedback. Separate from the FirstNet program, continued Federal investment in research labs, such as NIST and NTIA ITS, provides a strong, independent research foundation that benefits the broader communications ecosystem, including public safety.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TED CRUZ TO
CORY DAVIS

Question 1. Since 2015, the Commerce Department’s Inspector General (IG) has issued 19 audit and evaluation reports and two investigative reports on the FirstNet Authority highlighting modifications to the network contract that “made it easier for AT&T to achieve milestone compliance and payment,”¹ the Authority’s failure to “adequately assess contractor performance to ensure AT&T achieved” network coverage and device connections targets,² and conduct by senior leadership that “interfer[ed] with OIG’s statutory right of access and duty to keep the Secretary of Commerce and Congress informed of serious issues affecting [the] FirstNet Authority.”³ In August, the IG issued a report finding that senior FirstNet Authority officials obstructed oversight, withheld and altered documents, directed staff not to cooperate with the IG, and cultivated an internal “warlike” relationship with the oversight office, describing the IG as their “common enemy.”⁴ That same report also found retaliation against whistleblowers, including efforts to pressure at least one employee to resign, which led the IG to take the highly unusual step of making a criminal referral to the Department of Justice.

Other IG reports have raised serious questions about the Authority’s management of its contract with AT&T. In May 2024, the IG stated that the Authority “did not ensure . . . desired results for both coverage and device connection targets for each state and territory” were achieved due to the decision to “accept[] AT&T’s proposed nationwide coverage metrics” and “repeatedly chang[e] device connection target requirements from state-by-state to a less stringent nationwide basis.”⁵ Absent this, “AT&T would not have met the originally contracted state-by-state requirement for 34 states and one territory.”⁶ Follow up audits in June 2024 reinforced these findings.⁷

These reports raise questions about the Authority’s governance and its oversight of its contract with AT&T. Some have pointed to the Authority’s nebulous “independent” status in Federal statute as part of the reason for the lackluster accountability.

a. You testified that the FirstNet Authority “has frequently operated in a manner that blurs the line between a Federal oversight body and a commercial advocate for its vendor” and that the Authority’s independence “means it can largely operate free from accountability to NTIA officials.” Do you think eliminating the Authority’s independence and making it directly accountable to NTIA would address these concerns?

Answer. Verizon believes that giving NTIA direct authority over the work of the First Responder Network Authority would help alleviate these concerns. As I noted

¹Department of Commerce Office of Inspector General, *FirstNet Authority Did Not Ensure the Nation’s First Responders’ Needs Were Continuing to Be Met Timely When Modifying Key Objectives of the NPSBN Contract*, OIG–24–024–A (2024), <https://www.oig.doc.gov/OIGPublications/OIG-24-2.pdf>.

²Department of Commerce Office of Inspector General, *FirstNet Authority’s Lack of Contract Oversight for Device Connection Targets Puts the NPSBN at Risk of Impacting First Responders’ Use of the Network*, OIG–24–027–A (2024), <https://www.oig.doc.gov/wp-content/OIGPublications/OIG-24-027-A-REDACTED.pdf>; Department of Commerce Office of Inspector General, *FirstNet Authority’s Lack of NPSBN Contract Oversight for Coverage Puts at Risk First Responders’ Ability to Serve the Public Effectively*, OIG–24–026–A (2024), <https://www.oig.doc.gov/wp-content/OIGPublications/OIG-24-026-A-REDACTED.pdf>.

³Department of Commerce Office of Inspector General, *Investigation into Allegations That FirstNet Authority Senior Officials Interfered with OIG Audits*, OIG–24–0175 (2025), https://www.oig.doc.gov/wp-content/OIGPublications/Public_Investigative_Summary_24-0175_SECURED.pdf.

⁴*Id.*

⁵*Supra* note 1.

⁶*Id.*

⁷*Supra* note 2.

in my testimony, designating the Authority as an “independent entity” within NTIA without defining what that means has created confusion. And yes, the Authority has used this confusion to claim that it can largely operate free from accountability to NTIA officials, contrary to what NTIA recommends, and even without regard to larger Administration policy objectives. The Authority has frequently operated in a manner that blurs the line between a Federal oversight body and a commercial advocate for its vendor. This misalignment confuses state and local officials and distorts the marketplace.

But I want to be clear that eliminating the status of the Authority alone will not correct many of these problems. First, oversight without accountability will be ineffective. NTIA will need to have some mechanism to ensure that the Authority and ultimately the FirstNet contractor comply with NTIA mandates. And creating that accountability may mean further changes to the statute. For example, as I highlighted in my testimony, the law creating FirstNet includes language mandating that all funds not needed for the Authority’s administrative costs must be returned to the FirstNet contractor for reinvestment in “the network.” So, without reforms to the statute, NTIA may not legally be able to hold back funds for non-performance or issue penalties against the contractor for issues like those identified in the numerous OIG reports.

Second, simply subjecting the Authority to direct oversight without considering the respective roles of NTIA, the Board, and FirstNet employees may create oversight in name only. If the employees of FirstNet believe they answer to the Board, and the Board believes it is not answerable to NTIA, then very little may change with respect to the operations of FirstNet other than they can now claim that they have been affirmed by NTIA. In many ways eliminating the Authority’s independence without making clear what that means for how NTIA can oversee both future actions and certain critical past actions (like legal interpretations) of the Board would only reinforce the confusion that exists today. Similarly, clarifying how NTIA staff oversee and guide the actions of Authority employees would be helpful in creating more functional independence between the Authority and the FirstNet contractor.

Finally, we would see eliminating independence as just one step toward making FirstNet work for all of public safety. Verizon still would recommend that Congress consider other steps outlined in our testimony to make sure that multi-vendor competition is preserved and that non-FirstNet by AT&T subscribers can benefit from the FirstNet program.

Question 2. FirstNet arose out of a recommendation from the 9/11 Commission to establish a nationwide, interoperable network dedicated to public safety officials to achieve interoperability after communication failures on 9/11 meant firefighters, police officers, and other first responders couldn’t talk to one another because they were using incompatible radio systems. Does FirstNet, as it exists today, adequately address the concerns raised by, and recommendations from, the 9/11 Commission Report?

Answer. As I mentioned in my testimony, the challenges associated with interoperability between various public safety communications networks identified in the 9/11 Commission Report have largely been resolved through changes in technology and the competitive marketplace. But resolution of those challenges has been more of a function of transitioning public safety away from dedicated narrowband land mobile radio systems and onto wireless broadband networks built on international commercial standards. Certainly, FirstNet helped to advance that transition and create confidence in commercial networks as a substitute for dedicated public safety systems. But today, all major carriers offer a public safety broadband product that inherently interoperates with other networks.

But I worry that the robustness and reliability of public safety communications overall—which was an underlying concern in the 9/11 Commission Report—is being threatened. As I explained in my testimony, all networks have challenges, including those that were operating on 9/11. Public safety now ensures the reliability of their communications through the multi-vendor ecosystem, with contracts for secondary network vendors as well as partnerships with non-terrestrial communications providers. I think Congress, NTIA, and ultimately the FirstNet Authority should embrace this competition and not try to drive public safety to a single network solution. NTIA should incentivize network providers to improve the services they provide to first responders, and it should encourage first responders to choose the services that best meet their needs. Today, over half choose something other than AT&T’s FirstNet service. Congress must ensure the FirstNet Authority does not undercut fair competition by portraying itself as the “only” or even “preferred” solution. The inclusion of the U.S. Attorney General, the Secretary of Homeland Security, and the Director of the Office of Management and Budget (OMB) on the

FirstNet Board makes FirstNet's fair and unbiased operations even more important. More can be achieved by promoting a multi-network ecosystem, not by entrenching a monopoly. And Authority employees should not blur the line between government employees expected to exert oversight over the FirstNet contractor and sales people for what amounts to a commercial product.

Question 3. Congress authorized FirstNet in 2012, and the contract was awarded to AT&T in 2017. Since then, the communications sector has experienced massive technological advancements, including the transition from 4G LTE to 5G; the rise of satellite-based direct to cell technology; and new network management tools like network slicing and AI for dynamic management. Future developments—including 6G and dynamic spectrum sharing—are just around the corner.

a. Given modern communications technologies are built upon 3GPP standards that ensure interoperability, what is the continued need for a single nationwide network like FirstNet if the goal is to ensure interoperability?

i. Is there anything preventing first responders who today subscribe to, for example, Verizon Frontline wireless service, from texting, calling, or otherwise communicating with first responders who subscribe to T-Priority or FirstNet (other than potential differences in network coverage)? If not, then what interoperability concerns truly remain (land mobile radio notwithstanding)?

Answer. As I explained to the Committee, ensuring there is a single network used by all first responders is not only unnecessary to ensure effective public safety communications, it is contrary to achieving that goal. Multiple networks are important to ensuring that first responder needs are met, and AT&T's FirstNet network is certainly one of those networks. From a technological perspective, there is nothing preventing first responders today from communicating with one another across the three major wireless broadband public safety platforms—Verizon Frontline, T-Priority, and FirstNet by AT&T. All three of those networks provide public safety traffic with priority and pre-emption. That seamless exchange of traffic comes from building these public safety offerings on top of international 3GPP standards.

Question 4. Many public safety officials subscribe to multiple services, in addition to FirstNet, to achieve redundancy or coverage where FirstNet may be lacking. As part of a reauthorization effort, does Congress need to act to preserve this redundancy in the marketplace or will it exist sans legislative action?

Answer. You are correct that public safety today builds resiliency and redundancy into their communications solutions through subscribing to multiple vendors. We worry, though, that this multi-vendor ecosystem may come under threat over time. Today, well more than half of the public safety agencies in this country (and at least 48 percent of those in Texas) do not subscribe to FirstNet by AT&T. Yet they receive no direct benefit from the FirstNet program and cannot unless they abandon the communications solutions they believe best fit their needs. And increasingly we are seeing a blurring of the lines between the Authority as a Federal oversight body and Authority employees as commercial advocates for its vendor. True resiliency comes from redundancy and allowing first responders to choose communications solutions that meet their needs with open, fair competition among multiple vendors offering services across multiple platforms.

Verizon would propose, at minimum, that the Committee consider taking several actions as part of reauthorization to promote and protect this competitive environment. First, direct NTIA, as part of its public safety mission, to take concrete steps to foster competition and choice among public safety offerings, including eliminating any governmental bias in favor of any specific public safety network provider. For example, NTIA should encourage federal, state, and local agencies to have fully competitive communications service procurements, and the ability to sign up with multiple vendors. Second, NTIA should educate public safety officials about the broad availability of wireless solutions that provide services like priority and preemption for critical communications. Finally, Congress should include what would amount to a "technology and carrier neutrality" clause into the reauthorization, prohibiting the use of Federal grant funds to mandate a specific public safety communications provider.

More broadly, we think it would be important for Congress to recognize in a reauthorization that a multi-vendor ecosystem for public safety communications is essential for national and homeland security. A single point of failure for public safety communications should not be acceptable to Federal policymakers and the public at large. Local public safety officials deserve the right to choose the service that best meets their needs, and should benefit from the FirstNet program regardless of that choice. First responders collectively benefit from competition in a multi-network ecosystem, giving them the most resilient and reliable communications.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. JOHN THUNE TO
CORY DAVIS

Question. In the rise of the digital age, data breaches have compromised nationwide networks, violated consumer privacy, and emphasized the need to continually improve critical infrastructure. What reporting structures exist to notify FirstNet Authority and Congress of infrastructure breaches or workforce compliance failures?

Answer. Senator, I am unaware of any formal reporting structures that exist to notify the FirstNet Authority and Congress of such failures. Any reporting structures for the Authority would be included in the contract between the Authority and AT&T, which has been kept hidden from the public and policymakers. And as far as I know, there is nothing in the law that established the First Responder Authority that directs either AT&T or the Authority to provide mandatory reporting on any failures of any kind to Congress.

In fact, at present, the only way I know of that the public, Congress, or even NTIA is made aware of issues related to the Authority or AT&T as its contract partner is through the work of the Department of Commerce Office of Inspector General (OIG). Unfortunately, as I informed the Committee in my testimony, the Authority often serves as a marketing arm for AT&T's FirstNet brand and not as a governmental entity overseeing a government contract worth billions of dollars with AT&T.

And as I noted in my testimony, OIG has documented its concerns about operational questions related to the Authority, including whether it is meeting key network milestones, making justifiable investments into AT&T's network, and, most recently, silencing internal whistleblowers. OIG has also done important work exploring AT&T's network issues and the impact those issues had on AT&T's FirstNet customers. What OIG has identified are not merely administrative errors, but systemic risks that Congress should address because they directly impacted first responder readiness during disasters like the Maui wildfires.

As part of any reauthorization, Verizon would encourage Congress to consider the Authority's lack of oversight over AT&T and its FirstNet branded service. We would encourage Congress to consider providing NTIA with more direct authority over the operations of the Authority and the execution of the FirstNet contract by AT&T—a recommendation that also comes from public safety itself. The Authority has frequently operated in a manner that blurs the line between a Federal oversight body and a commercial advocate for its vendor. This misalignment confuses state and local officials and distorts the marketplace. Clearer oversight responsibilities for NTIA, with commensurate authority to create accountability and promote competition in the public safety marketplace, would give public safety additional confidence that the legal interpretations and practical actions of the Authority have undergone the appropriate level of scrutiny.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. DAN SULLIVAN TO
CORY DAVIS

Industry Best Practices:

Verizon Frontline also supports public safety in remote and disaster-prone areas, offering a useful comparison for best practices.

Question. From your perspective, what best practices should be required to ensure deployable public safety assets are exercised, logistics-tested, and deployment-ready in remote environments?

Answer. Our 30-year relationship with public safety means that we should do everything possible to make sure all Verizon Frontline assets, including our fleet of over 3,000 deployables, are ready whenever they are needed. We conduct "blue sky" planning exercises with our public safety partners around the country to help plan for how we collectively respond to emergency situations, including where/when/how we would utilize deployables in those operations. And within Verizon, we constantly check our Frontline assets to make sure that they are ready to go when needs arise and we refresh that fleet on a regular basis to be sure that we have the right cutting-edge communications assets in our deployable fleet. For those disasters where we have effective lead time to prepare, we work with federal, state, and local public safety officials to pre-stage deployable assets to accelerate response time. We also take that opportunity to verify that deployables identified for that response are ready in all respects for the job.

Our public safety partners need to be able to focus on effective "gray sky" disaster response when lives are on the line; they count on us to back them up with communications assets that are ready to go at a moment's notice. Every disaster creates

complications in communications response, so preparation and planning are essential.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARIA CANTWELL TO
CORY DAVIS

Salt Typhoon Impact. Last June, I wrote to AT&T's CEO requesting information to understand how the unprecedented Salt Typhoon attack impacted not only AT&T's commercial network but also whether the FirstNet network was affected as well.

I asked for the third-party threat assessments that would supposedly verify their claim that their networks were now secure from the next Chinese cyber attack. But AT&T has chosen not to cooperate.

I made the same request of Verizon and also didn't receive anything. In the face of increasingly sophisticated attacks like Chinese state-sponsored Salt Typhoon, public safety users should have confidence that the network they are using is secure and protected.

Question 1. Did the Salt Typhoon attacks penetrate Verizon's Frontline network, yes or no?

Answer. Verizon Frontline, our public safety communications service, rides on top of Verizon's commercial wireless network infrastructure. AT&T's FirstNet service and T-Mobile's T-Priority service operate in a similar way. To the extent that the attack penetrated our network, as with other providers, such penetration potentially affected both commercial and Verizon Frontline services. However, our investigation into the incursion uncovered no information indicating that the attackers targeted the Frontline service. Further, none of the individual numbers specifically targeted by Salt Typhoon (*i.e.*, the group of high-level government officials) were subscribed to the Frontline service.

Question 2. If no, is there a third-party assessment that confirms this? If so, do you commit to giving me that document?

Answer. We saw no indication that the Frontline service or its subscribers were specific targets of the Salt Typhoon attack, so our third-party assessor did not mention Frontline in its review. With your concerns in mind, we would like to have our Chief Information Security Officer brief you or your staff about the incursion and our work to contain it.

Question 3. If the Salt Typhoon attackers did penetrate the Frontline network, is there a third-party assessment confirming they have been fully evicted? If so, do you commit to giving me that document?

Answer. We have seen no evidence of the threat actor being present in our networks since October 9, 2024. Further, we have not been alerted by any Federal agency that they have seen evidence of activity in our network since that time. With respect to the second part of your question, please see our answers above.

Question 4. Has Mandiant or another third-party identified any network vulnerabilities, on Frontline or otherwise, exploited by Salt Typhoon attackers that Verizon has not fully remediated, yes or no?

Answer. Please see our answers above.

Question 5. Has Mandiant or another third-party made any security recommendations that Verizon has not fully implemented on the Frontline network, yes or no? This includes, but is not limited to, patching network edge devices such as VPNs, firewalls, and routers, and implementing phishing-resistant multi-factor authentication.

Answer. Please see our answers above.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN HICKENLOOPER TO
CORY DAVIS

Federal Labs. Colorado is home to many Federal labs which perform mission critical research, development, and testing to improve communications service. The First Responder Network Authority, the NTIA's Institute for Telecommunications Sciences (ITS), and NIST's Public Safety Communications Research Division within the Communications Technology Laboratory all call Boulder, Colorado their home. The FirstNet Authority's lab in Boulder tests public safety technologies which will be used by first responders. NTIA's ITS lab is the gold standard for researching how to maximize spectrum efficiency and reduce interference to Federal agency missions and commercial radiofrequency applications. NIST's PSCR Division supports the de-

velopment of technical specifications to advance next-generation communications technologies.

Question 1. Do you believe the research activities performed by the NIST, NTIA, and FirstNet Authority Labs are key to the success of advancing the state of the art in public safety communications? Which areas of research or technical challenges in public safety communications may be useful to examine going forward?

Question 2. 47 U.S.C. § 1443 outlines a process for public safety wireless communications research and development. Do you believe the FirstNet Authority could strengthen its collaboration with nearby NIST and NTIA ITS labs with respect to public safety communications research? If yes, please elaborate on how this collaboration could be strengthened.

Question 3. Would you support or oppose cuts to Federal funding to labs, including the aforementioned labs, which support the advancement of communications research?

Question 4. The Public Safety Trust Fund was only authorized until Fiscal Year 2022. From your perspective, describe where additional Federal resources may be needed for public safety communications research.

Answer. Senator, I believe the public and private sectors both have key roles to play in advancing public safety communications. As I testified before the Committee, Verizon is on the leading edge of advancing public safety communications through technologies like 5G network slicing. We also sponsor the Verizon Frontline Innovation Program. The Verizon Frontline Innovation Program is a first-of-its-kind innovation incubator dedicated to creating 5G-enabled solutions for public safety, as well as connectivity solutions in austere network deprived environments. The program explores new, innovative technologies that provide solutions to public safety agencies. To date, we have worked with over 25 Innovation Partners to evaluate existing products or to ideate on new solutions.

Federal labs similarly help to advance critical public safety technologies. I would defer to Congress on questions like the appropriate level of funding for various labs funded by the Federal government. But as I noted in my recent testimony, Verizon Frontline is the public safety market leader while AT&T's FirstNet service currently serves less than half of the public safety communications marketplace. Government funding can certainly be helpful in advancing public safety communications, but to the extent that Congress is considering additional investments in this area, those investments should support research that helps *all* of public safety, and not just AT&T customers. Research funded by the Federal government should be open to all public safety communications providers, and NIST should be committed to working with all network providers on a fair and unbiased basis. In reauthorizing the FirstNet Authority, Congress should ensure that NIST's public safety research programs and any associated funding are not conducted in a manner that is open only to the FirstNet Authority lab or conducted solely for the benefit of AT&T's FirstNet customers.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARIA CANTWELL TO
MEL MAIER

Salt Typhoon Impact. Last June, I wrote to AT&T's CEO requesting information to understand how the unprecedented Salt Typhoon attack impacted not only AT&T's commercial network but also whether the FirstNet network was affected as well.

I asked for the third-party threat assessments that would supposedly verify their claim that their networks were now secure from the next Chinese cyber attack. But AT&T has chosen not to cooperate.

I made the same request of Verizon and also didn't receive anything.

In the face of increasingly sophisticated attacks like the Chinese state-sponsored Salt Typhoon, public safety users should have confidence that the network they are using is secure and protected.

Question 1. Mr. Maier, do you think that we need stronger cybersecurity protections for FirstNet and other networks that first responders rely on?

Answer. Strong cybersecurity protections for FirstNet and other networks that first responders rely on are essential. As these systems become more complex and interconnected, the number of possible entry points for cyber threats increases, making cybersecurity an increasingly important consideration.

FirstNet's dedicated public safety core, oversight, and built-in security measures are specifically designed to protect both the network and the sensitive information it carries. In addition, input from the Public Safety Advisory Committee helps en-

sure that real-world threats and experiences from public safety agencies that have faced these challenges inform network decisions and improvements. Any disruption or loss of trust in the network could directly impact emergency response, so maintaining a secure, reliable, and resilient system must remain a top priority.

First Responder Use of other Networks. Our wireless networks have become critical infrastructure, and when they fail, the consequences for public safety can be severe. Just last month, Verizon experienced an outage lasting roughly ten hours. Emergency management systems in Washington, D.C., and New York City had to issue alerts telling residents to find other ways to reach 911.

In February 2024, AT&T suffered a nationwide outage that blocked over 92 million voice calls and more than 25,000 calls to 911 centers—and knocked out service for FirstNet subscribers. On Christmas Day 2020, a bombing in Nashville took out an AT&T facility, causing regional outages that left FirstNet subscribers without service for hours. The Nashville Police Department had to scramble for backup phones from Verizon.

Question 1. Mr. Maier, we've heard that many public safety agencies subscribe to multiple wireless services rather than relying solely on FirstNet. Why is that?

Answer. Public safety agencies select wireless services based on myriad factors, including which coverage and services best meet their operational needs. These decisions often consider coverage capabilities within their jurisdictions, cost, past contractual relationships, and several other factors. An agency may need to contract with multiple providers to achieve comprehensive coverage across its entire service area, based on each provider's tower locations. Some agencies also rely on overlapping coverage from multiple vendors to ensure redundancy and resiliency.

Question 2. Mr. Maier, we've heard that FirstNet and Verizon failed to clearly communicate with first responders that their networks were down. Should first responders receive faster, more reliable notification when there's an outage affecting their network?

Answer. Having timely and actionable information about network outages is critically important for public safety agencies, so they can take steps to mitigate the impact of an outage on the public. One of FirstNet's strengths is the transparency built into its governance and operations. After the 2024 FirstNet outage, public safety demanded accountability with briefings provided to the Board and PSAC, and the FirstNet Authority directed AT&T to do an after-action and organized a task force to identify recommendations for improvement. One of the primary improvements has been to communications.

FirstNet Central was refined to enhance outage notifications. FirstNet Central provides agencies with detailed visibility into network status, including deployables and county-level outages, a feature that was requested directly by the public safety community. FirstNet is the only network that provides full visibility into coverage, tower locations, outages, maintenance information, and the location of deployable assets through this portal.

Public safety needs this kind of visibility into every outage, regardless of provider. That is why APCO has urged the Federal Communications Commission (FCC) to amend the rules regarding how service providers must notify 9-1-1 centers about network outages that impact the ability of the public to reach 9-1-1. APCO, along with other 9-1-1 associations, has requested that the FCC revise its rules so that these notifications are provided in a format that is easily accessible to 9-1-1 center personnel and provide real-time, actionable information. Specifically, APCO has advocated for a secure, two-way centralized portal for service providers to update with information regarding network status, geographic areas experiencing service disruptions, and restoration efforts, and that 9-1-1 center personnel could access for real-time situational awareness when outages occur. This request is still pending with the FCC.

Competition. When Congress authorized FirstNet in 2012, it was clear that the commercial telecommunications market wasn't going to deliver the kind of priority service public safety needed without help from the Federal Government.

Now, nearly ten years after AT&T received the FirstNet contract, competitors like Verizon and T-Mobile have emerged with their own public service offering.

Question 1. How does competition in the marketplace improve service for public safety officials?

Answer. Competition in the marketplace can drive innovation, improve service, and expand options for public safety agencies. FirstNet was created to address mission-critical needs that were not being met by the commercial marketplace alone. FirstNet, built using common commercial standards, has driven the modernization of public safety technology and has galvanized competition in public safety offerings.

Before FirstNet was created, the average consumer had better cell phone technology than a first responder in the field. Now we have FirstNet, and additional public safety offerings like Verizon Frontline and T-Priority. FirstNet is specifically built to address public safety needs and expectations. As a result, competitors seeking to similarly serve the public safety community must meet comparable standards, which drives increased reliability, security, and innovation across the marketplace. Overall, competition benefits all public safety users, whether they are FirstNet customers or not, by fostering modernization and improving the technology and services available to agencies.

Question 2. Does having alternate service offerings help public safety officials in planning and redundancy?

Answer. Having alternate service offerings strengthens public safety planning efforts and helps ensure redundant communications networks. By delivering services aligned with public safety's operational requirements, FirstNet has spurred competition among other providers, which has, in turn, given public safety agencies multiple service offerings to incorporate into their planning. This flexibility enables public safety agencies to leverage different infrastructure, devices, and capabilities to maintain continuity of service, address local coverage needs, and avoid single points of failure.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN HICKENLOOPER TO
MEL MAIER

Federal Labs. Colorado is home to many Federal labs which perform mission critical research, development, and testing to improve communications service. The First Responder Network Authority, the NTIA's Institute for Telecommunications Sciences (ITS), and NIST's Public Safety Communications Research Division within the Communications Technology Laboratory all call Boulder, Colorado their home. The FirstNet Authority's lab in Boulder tests public safety technologies which will be used by first responders. NTIA's ITS lab is the gold standard for researching how to maximize spectrum efficiency and reduce interference to Federal agency missions and commercial radiofrequency applications. NIST's PSCR Division supports the development of technical specifications to advance next-generation communications technologies.

Question 1. Do you believe the research activities performed by the NIST, NTIA, and FirstNet Authority Labs are key to the success of advancing the state of the art in public safety communications? Which areas of research or technical challenges in public safety communications may be useful to examine going forward?

Answer. The research activities performed by NIST, NTIA, and the FirstNet Authority Labs are important to advancing public safety communications. NIST and PSCR have supported public safety's broadband evolution since 2005, including co-ordination with the FirstNet Authority and work at the Boulder Laboratories. This research helps ensure public safety communications evolve using common standards and reflect real-world operational needs.

These efforts are especially valuable because they look ahead to future challenges. Research into areas such as Supplemental Coverage from Space, 6G, network sensing, and the integration of AI and machine learning can improve resiliency, security, and flexibility in wireless networks.

Question 2. 47 U.S.C. § 1443 outlines a process for public safety wireless communications research and development. Do you believe the FirstNet Authority could strengthen its collaboration with nearby NIST and NTIA ITS labs with respect to public safety communications research? If yes, please elaborate on how this collaboration could be strengthened.

Answer. APCO supports collaboration and information sharing across Federal research organizations to advance public safety communications. Public safety benefits when research is focused on common goals to advance reliable, secure, and effective communications for first responders. We defer to the FirstNet Authority, NTIA, and NIST with respect to the manner and means by which this collaboration takes place.

Question 3. Would you support or oppose cuts to Federal funding to labs, including the aforementioned labs, which support the advancement of communications research?

Answer. Public safety communications research helps ensure that first responders rely on modern, fully tested, and mission-ready equipment before deployment. Federal labs can serve a critical role in developing, evaluating, and validating tech-

nologies that support public safety communications. We respectfully defer to Congress regarding specific Federal funding allocations.

Question 4. The Public Safety Trust Fund was only authorized until Fiscal Year 2022. From your perspective, describe where additional Federal resources may be needed for public safety communications research.

Answer. We defer to NTIA, NIST, and the FirstNet Authority regarding the allocation of their Federal resources, as these entities are best positioned to determine research priorities. That said, continued research will be critical as the public safety community transitions to NG9-1-1 and other modern communications capabilities, including broadband, satellite services, AI, and other emerging technologies. This research provides valuable insights that guide the development and deployment of advanced public safety communications technologies and can help identify additional areas for Federal investment to support public safety. For example, Federal funding is vital to modernize 9-1-1 centers and transition them to NG9-1-1, ensuring public safety agencies have secure, reliable, and interoperable communications systems.

