# 20 YEARS AFTER 9/11: EXAMINING EMERGENCY COMMUNICATIONS

## HEARING

BEFORE THE

## SUBCOMMITTEE ON EMERGENCY PREPAREDNESS, RESPONSE, AND RECOVERY

OF THE

## COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

OCTOBER 7, 2021 and NOVEMBER 2, 2021

**Serial No. 117–32**

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
46–622 PDF WASHINGTON : 2022

## COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
DONALD M. PAYNE, JR., New Jersey
J. LUIS CORREA, California
ELISSA SLOTKIN, Michigan
EMANUEL CLEAVER, Missouri
AL GREEN, Texas
YVETTE D. CLARKE, New York
ERIC SWALWELL, California
DINA TITUS, Nevada
BONNIE WATSON COLEMAN, New Jersey
KATHLEEN M. RICE, New York
VAL BUTLER DEMINGS, Florida
NANETTE DIAZ BARRAGÁN, California
JOSH GOTTHEIMER, New Jersey
ELAINE G. LURIA, Virginia
TOM MALINOWSKI, New Jersey
RITCHIE TORRES, New York
JOHN KATKO, New York
MICHAEL T. MCCAUL, Texas
CLAY HIGGINS, Louisiana
MICHAEL GUEST, Mississippi
DAN BISHOP, North Carolina
JEFFERSON VAN DREW, New Jersey
RALPH NORMAN, South Carolina
MARIANNETTE MILLER-MEEKS, Iowa
DIANA HARSHBARGER, Tennessee
ANDREW S. CLYDE, Georgia
CARLOS A. GIMENEZ, Florida
JAKE LATURNER, Kansas
PETER MEIJER, Michigan
KAT CAMMACK, Florida
AUGUST PFLUGER, Texas
ANDREW R. GARBARINO, New York

HOPE GOINS, *Staff Director*
DANIEL KROESE, *Minority Staff Director*
NATALIE NIXON, *Clerk*

---

## SUBCOMMITTEE ON EMERGENCY PREPAREDNESS, RESPONSE, AND RECOVERY

VAL BUTLER DEMINGS, Florida, *Chairwoman*

SHEILA JACKSON LEE, Texas
DONALD M. PAYNE, JR., New Jersey
AL GREEN, Texas
BONNIE WATSON COLEMAN, New Jersey
BENNIE G. THOMPSON, Mississippi *(ex officio)*
KAT CAMMACK, Florida, *Ranking Member*
CLAY HIGGINS, Louisiana
MARIANNETTE MILLER-MEEKS, Iowa
ANDREW R. GARBARINO, New York
JOHN KATKO, New York *(ex officio)*

LAUREN MCCLAIN, *Subcommittee Staff Director*
DIANA BERGWIN, *Minority Subcommittee Staff Director*
AARON GREENE, *Subcommittee Clerk*

# CONTENTS

# 20 YEARS AFTER 9/11: EXAMINING EMERGENCY COMMUNICATIONS, PART I

**Thursday, October 7, 2021**

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON EMERGENCY PREPAREDNESS,
RESPONSE, AND RECOVERY,
*Washington, DC.*

The subcommittee met, pursuant to notice, at 12:04 p.m., via Webex, Hon. Val Butler Demings [Chairwoman of the subcommittee] presiding.

Present: Representatives Demings, Jackson Lee, Payne, Green, Watson Coleman, Cammack, Higgins, and Miller-Meeks.

Also present: Representative Slotkin.

Mrs. DEMINGS. The Subcommittee on Emergency Preparedness, Response, and Recovery will come to order.

The subcommittee is meeting today to receive testimony on "20 Years After 9/11: Examining Emergency Communications."

Without objection, the Chair is authorized to declare the subcommittee in recess at any point.

Last month, our Nation marked 20 years since the worst terrorist attack on U.S. soil. The Committee on Homeland Security joined many of our colleagues from New York and New Jersey to visit the National September 11 Memorial and Museum, and held a roundtable with first responders. We have also conducted several hearings on the evolution of the Department of Homeland Security and heard from our intelligence community regarding the current and emerging threats to our homeland.

Today, the Emergency Preparedness, Response, and Recovery Subcommittee will examine the progress made in emergency communications since September 11, 2001, and discuss the challenges that may still persist today.

As you know, from emergency managers and first responders who served on September 11 and the 9/11 Commission Report, police officers, firefighters, and emergency medical services experienced significant problems communicating within their own agencies and with others who responded on that day.

On the morning of September 11, I was assigned to the Orlando International Airport as the commander of the Orlando Police Department Airport Police Division. As reports of the attack on the World Trade Center emerged and the Federal Aviation Administration ordered all aircraft grounded, airport and law enforcement leadership had to immediately execute emergency operations to protect passengers, employees, and the public.

I know how the first responders felt in Orlando. I can't even begin to imagine all that the first responders on the ground experienced and went through in New York. My husband served in law enforcement as well, and I have two sons who are firefighters. My heart continues to go out to the families who lost loved ones that tragic day.

Communications and interoperability are essential. First responders consider it their lifeline.

Over the next months and years, incredible progress has been made to address the undescribable challenges on September 11 and improve the Nation's emergency communications apparatus through programs such as First Responder Network Authority and the Integrated Public Alert and Warning System. However, challenges in operability and interoperability still persist, and our aging 9–1–1 infrastructure poses additional vulnerabilities.

Operability and interoperability remain among the greatest concerns that first responders and public safety officials face. Tragedy and disaster can come, as we all know, in many forms.

Climate change also poses significant and growing challenges for emergency communications. From rapid-spreading wildfires in the West to increasingly strong and frequent hurricanes, cell towers and radio communications systems remain vulnerable to critical failures. In August, Hurricane Ida, a powerful Category 4 storm, crashed the New Orleans, Louisiana, 9–1–1 call center and FirstNet Authority, making it difficult, if not impossible, to respond to emergencies.

Members of Congress, we know we have an important role in the improvement of emergency communications technology. We must continue to provide funding through grants, such as the State Homeland Security Program and the Urban Area Security Initiative. These programs have provided critical Federal funding for jurisdictions to buy equipment, build and fix communications towers, and make broadband improvements.

While grant programs such as UASI are created specifically for urban areas, we understand that rural communities and Tribal lands face their own challenges with broadband and connectivity that can also complicate emergency response. Federal grants support these communities, but can always be more robust to meet the needs more completely.

Though communications, interoperability, and resilient infrastructure are priorities for emergency and first responders, the public may only experience their benefit or challenges during times of crisis. Today's hearing will serve as an important forum to understand the current state of emergency communications systems and any gaps that may still persist.

I am grateful today for the participation of our witnesses, and I look forward to your testimony.

[The statement of Chairwoman Demings follows:]

STATEMENT OF CHAIRWOMAN VAL DEMINGS

OCTOBER 7, 2021

Last month, our Nation marked 20 years passed since the worst terrorist attacks on U.S. soil. The Committee on Homeland Security joined many of our colleagues from New York and New Jersey to visit the National September 11 Memorial & Mu-

seum and held a roundtable with first responders. We have also conducted several hearings on the evolution of the Department of Homeland Security and heard from our intelligence community regarding the current and emerging threats to our homeland.

Today, the Emergency Preparedness, Response, and Recovery Subcommittee will examine the progress made in emergency communications since September 11, 2001 and discuss the challenges that may persist today. As we know from emergency managers and first responders who served on September 11 and the 9/11 Commission Report, police officers, firefighters, and emergency medical services experienced significant problems communicating within their own agencies and across all who responded that day.

On the morning of September 11, I was serving as the Orlando Police Department's captain of the division stationed at the Orlando International Airport. As reports of the attack on the World Trade Center emerged and the Federal Aviation Administration ordered all aircraft grounded, airport and law enforcement leadership had to immediately execute emergency operations to protect passengers, employees, and the public. Further, given the location and runway length, the airport became a safe harbor for aircraft to land in compliance with FAA orders. Communications and interoperability were essential to our ability to keep the public safe that day.

Over the next months and years, incredible strides were made to address the system failure on September 11 and improve the Nation's emergency communications apparatus through programs such as the First Responder Network Authority (FirstNet Authority) and the Integrated Public Alert & Warning System (IPAWS). However, challenges in operability and interoperability still persist, and our aging 9–1–1 infrastructure poses additional vulnerabilities.

Operability and interoperability remain among the greatest concerns that first responders and public safety officials face. During the 9/11 attacks, due to insufficient technology police officers and firefighters were unable to communicate among themselves and with each other, delaying response efforts. I know first-hand how valuable every second is when responding to an emergency and that being unable to get in touch with fellow officers can have detrimental consequences.

Climate change also poses significant and growing challenges for emergency communications. From rapid-spreading wildfires in the West to increasingly strong and frequent hurricanes, cell towers and radio communications systems remain vulnerable to critical failures. In August, Hurricane Ida, a powerful Category 4 storm, crashed the New Orleans, Louisiana 9–1–1 call center and FirstNet Authority, making it difficult, if not impossible to respond to emergencies.

Members of Congress have an important role in the improvement of emergency communications technology. We must continue to provide funding through grants such as the State Homeland Security Program and the Urban Area Security Initiative (UASI). These programs have provided critical Federal funding for jurisdictions to buy equipment, build and fix communications towers, and make broadband improvements.

While grant programs such as UASI are created specifically for urban areas, rural communities and Tribal lands face their own challenges with broadband and connectivity that can also complicate emergency response. Federal grants support these communities but can always be more robust to meet the needs more completely. Though communications, interoperability, and resilient infrastructure are priorities for emergency and first responders, the public may only experience their benefit—or challenges—during times of crisis. Today's hearing will serve as an important forum to understand the current state of emergency communications systems and any gaps that may persist.

Mrs. DEMINGS. The Chair now recognizes the Ranking Member of the subcommittee, the gentlewoman from Florida, Mrs. Cammack, for an opening statement.

Mrs. CAMMACK. Well, thank you, Chairwoman Demings. I appreciate your leadership on this issue. As we have said many times before, we are extremely lucky that Florida has two, two leaders that are focused on our first responders, emergency preparedness, and have extremely personal ties to this. So thank you again for convening this important hearing today on our first responder communications.

As we all know, first responders play an invaluable role in communities across America, and ensuring that they have the necessary training, equipment, funding, and resources is a top priority. I look forward to working with the Chairwoman to address some of the challenges currently facing our first responders, an issue I know that she also cares very deeply about.

Now, last month, we mourned the 20th anniversary of the September 11 attacks. The 9/11 Commission Report, which recounts events surrounding that tragic day, calls attention to the fact that the lack of communication among emergency personnel, 9–1–1 communication call centers, and individuals in the towers caused confusion, ultimately costing lives.

One New York fire department chief who was stationed in the North Tower is quoted in the report as saying, "people watching on TV certainly had more knowledge of what was happening 100 floors above us than we did in the lobby. Without critical information coming in, it is very difficult to make informed, life-saving, critical decisions."

I have said this before. My own husband, Matt, he became a firefighter in part because of 9/11, watching 343 men and women run into the towers to save their community members, their neighbors, their coworkers. I can't imagine as the wife of a first responder what it would be like to witness in real time a lack of communication on the ground.

Now, fast-forward, after first responders experienced similar communication challenges during Hurricane Katrina in 2005, Congress passed the Post-Katrina Emergency Management Reform Act. This legislation took significant steps to standardize emergency communications across the country by establishing the National Emergency Communications Plan. Now, as a result of the work accomplished by the NECP, a survey conducted in 2018 found that 84 percent of State and territorial respondents reported significant or some improvement in the strengthening of their communications operability.

The Post-Katrina Emergency Management Reform Act also helped provide State and local first responders with access to grant funding to develop and implement State-wide communication interoperability plans to enhance interoperable communications for public safety and officials at all levels of government.

In 2012, Congress took an additional step to improve our Nation's emergency communication network by passing the Middle Class Tax Relief and Job Creation Act. This legislation established the first responder network authority, also known as FirstNet, which is responsible for overseeing the build-out and operation of a Nation-wide interoperable public safety broadband network. This dedicated public safety network has been critical in ensuring that, during a disaster, necessary information is able to reach first responders on the ground.

While both the Post-Katrina Emergency Management Reform Act and the Middle Class Tax Relief and Job Creation Act made significant improvements to emergency communications, many challenges still remain. One such challenge facing first responder networks is the very real threat of a cyber attack. In fact, a recent survey conducted by SAFECOM found that over a third of organi-

zations indicated that cybersecurity incidents have had an impact on the ability of their emergency response providers and Government officials' ability to communicate over the past 5 years.

The study also found that fire departments and organizations located in rural areas tend to be the least prepared for cybersecurity attacks, with 62 percent of fire departments indicating that they do not conduct any cybersecurity planning. Over 55 percent of organizations surveyed indicated that lack of funding is the reason that they do not and cannot invest in cybersecurity.

First responders in rural areas like Putnam County, one of my counties in my district, oftentimes do not have the necessary funding to update their technology, and even when they are able to secure the necessary funds, the technology can be unreliable because of a lack of coverage. However, while advances in technology may lead to increases in cyber attacks, technological innovation can also be revolutionary.

Next Generation 9–1–1 enhances the capabilities of today's 9–1–1 networks, allowing compatibility with more types of communication to provide greater situational awareness to dispatchers and emergency responders. Next Generation 9–1–1 will enable 9–1–1 call centers to accept and process voice calls, video, photos, and text message from responders and the public. This capability really could be a game changer for those in need and for those responding to the call.

As we continue to work to address the challenges facing emergency communications networks to improve the capabilities across the board, we must work to ensure that we are not pursuing a one-size-fits-all approach that may not accommodate the unique needs that many of our communities face, especially those in rural communities.

I applaud the progress that has been made to improve first responder communications over the last 20 years, but we have a long way to go. In preparation for today's hearing, I actually spoke with several of my sheriffs, fire chiefs, and emergency managers. Coming from a rural district, several said we are no better today than we were 20 years ago.

So, today, I look forward to hearing from our witnesses on what additional steps we in Congress can take to ensure that our first responders have the information and connectivity to continue serving our communities.

With that, Madam Chairwoman, I yield back.

[The statement of Ranking Member Cammack follows:]

STATEMENT OF RANKING MEMBER KAT CAMMACK

I would like to thank Chairwoman Demings for convening this important hearing today on first responder communications.

First responders play an invaluable role in communities across America and ensuring they have the necessary training, equipment, funding, and resources is a top priority of mine. I look forward to working with the Chairwoman to address some of the challenges currently facing our first responders, an issue I know she also cares very deeply about.

Last month, we mourned the 20th anniversary of the September 11 attacks. The 9/11 Commission report, which recounts events surrounding that tragic day, calls attention to the fact that lack of communication among emergency personnel, 9–1–1 call centers, and individuals in the towers sowed confusion, ultimately costing lives. One FDNY chief who was stationed in the North Tower is quoted in the report as saying, "people watching on TV certainly had more knowledge of what was hap-

pening a hundred floors above us than we did in the lobby . . . [W]ithout critical information coming in . . . it's very difficult to make informed, critical decisions."

After first responders experienced similar communication challenges during Hurricane Katrina in 2005, Congress passed the Post-Katrina Emergency Management Reform Act (PKEMRA). This legislation took significant steps to standardize emergency communications across the country by establishing the National Emergency Communications Plan (NECP). As a result of the work accomplished by the NECP, a survey conducted in 2018 found that 84 percent of State and territorial respondents reported significant or some improvement in the strengthening of their communications operability.

PKEMRA also helped provide State and local first responders with access to grant funding to develop and implement State-wide Communication Interoperability Plans to enhance interoperable communications for public safety and officials at all levels of government.

In 2012, Congress took additional steps to improve our Nation's emergency communication networks by passing the Middle Class Tax Relief and Job Creation Act. This legislation established the First Responder Network Authority (FirstNet), which is responsible for overseeing the build-out and operation of a Nation-wide interoperable public safety broadband network. This dedicated public safety network has been critical in ensuring that during a disaster, necessary information is able to reach first responders on the ground.

While both PKEMRA and the Middle Class Tax Relief and Job Creation Act made significant improvements to emergency communications, many challenges still remain.

One such challenge facing first responder networks is the very real threat of a cyber attack. In fact, a recent survey conducted by SAFECOM found that, "over a third of organizations indicated that cybersecurity incidents have had an impact on the ability of their emergency response providers and government officials' ability to communicate over the past 5 years."

The study also found that, "fire departments and organizations located in rural areas tend to be least prepared for cybersecurity attacks [ . . . ] with 62 percent of fire departments indicating that they do not conduct any cybersecurity planning." And over 55 percent of organizations surveyed indicated that lack of funding is the reason that they do not invest in cybersecurity.

First responders in rural areas, like Putnam County, Florida, oftentimes do not have the necessary funding to update their technology, and even when they are able to secure the necessary funds, the technology can be unreliable because of lack of coverage.

However, while advances in technology may lead to increases in cyber threats, technological innovations can also be revolutionary. Next Generation 9–1–1 enhances the capabilities of today's 9–1–1 networks allowing compatibility with more types of communication to provide greater situational awareness to dispatchers and emergency responders. Next Generation 9–1–1 will enable 9–1–1 call centers to accept and process voice calls, video, photos, and text messages from responders and the public. This capability could really be a game-changer—for those in need, and those responding to the call.

As we continue to work to address the challenges facing emergency communications networks, to improve capabilities across the board, we must work to ensure that we are not pursuing a one-size-fits-all approach that may not accommodate the unique needs of many first responders, especially those in rural communities.

I applaud the progress that has been made to improve first responder communications in the past 20 years and look forward to hearing from our witnesses today on what additional steps are needed to ensure first responders have the information and connectivity to continue serving our communities.

Mrs. DEMINGS. I want to thank the Ranking Member.

Members are also reminded that the subcommittee will operate according to the guidelines laid out by the Chairman and Ranking Member in their February 3 colloquy regarding remote procedures.

Without objection, Members not on the subcommittee shall be permitted to sit and question the witnesses. Additional Member statements may be submitted for the record.

[The statement of Chairman Thompson follows:]

STATEMENT OF CHAIRMAN BENNIE G. THOMPSON

OCTOBER 7, 2021

Twenty years ago, on 9/11, we suffered the deadliest terrorist attack in our Nation's history. During this unprecedented attack, our brave first responders did their best to locate and rescue survivors and many lives were saved because of their heroism. Unfortunately, their heroic efforts to rescue survivors were hampered by communications challenges.

The 9/11 Commission's investigation found that first responders were forced to make life-and-death decisions based on poor communications. Unable to connect with one another, neither the supporting agencies nor the rescuers themselves could coordinate effectively to help victims. Systems were overloaded, and 9–1–1 call centers placed victims on hold multiple times. Operators faced a "lack of awareness" about what was happening at the World Trade Center and were overwhelmed by the volume of incoming calls. In short, 9/11 revealed fundamental problems with communications systems used by first responders and public safety officials.

Since then, we have made great strides in technology and capabilities, including the creation of Integrated Public Alert and Warning System (IPAWS), the First Responder Network Authority (FirstNet Authority), and Next Generation 9–1–1 (NG 911). However, two decades later, several emergency communications challenges remain, including, interoperability issues, network outages, and challenges with FirstNet Authority.

On December 25, 2020, a bomb was detonated downtown in Nashville, Tennessee, interrupting 66 emergency communications districts for more than 97 hours. The AT&T hub was one of the buildings blasted during the bombing, forcing failure of the generators, and causing a loss of 9–1–1 communications for 4 days. A major issue in these situations is that generators are often the back-up solution for when a major disaster renders communication towers inoperable, but it may take days to reach an area ravaged by storm or explosion, leaving lives at risk. While we continue to protect our Nation against threats posed by foreign and domestic terrorist organizations, we also must ensure adequate focus and funding to end communication infrastructure challenges.

Department of Homeland Security preparedness grants such as Urban Security Initiative (UASI) and State Homeland Security Program (SHSP) serve as an important source of funds for first responders and public safety officials. It allows them to use funding for expenses such as communications equipment, planning, training, and exercises. As the threats to our Nation continue to evolve, we must strengthen our communication systems to better protect our Nation from potential threats. I look forward to hearing from our witnesses today about the communication challenges we face and what we can do to aid them in making our communities safer.

Mrs. DEMINGS. It is now my honor to welcome our panel of witnesses.

Our first witness is Dr. Chris Rodriguez. Dr. Rodriguez is the director of the Homeland Security Emergency Management Agency for the District of Columbia, where he serves as the Homeland Security advisor and State coordinating officer. Dr. Rodriguez serves as the State administrative agent for all Homeland Security Federal grant funding for the district and the National Capital region.

Prior to his current role, Dr. Rodriguez served as the director of New Jersey's Office of Homeland Security and Preparedness from 2014 to 2017. Dr. Rodriguez also serves as a senior analyst in the Central Intelligence Agency's Counterterrorism Center following the attacks of September 11.

Dr. Rodriguez, thank you so much for joining us.

The Chair now recognizes the gentlewoman from Michigan, Ms. Slotkin, to introduce our second witness.

Ms. SLOTKIN. Great. Thank you so much, Madam Chair, for letting me do a little cameo here. I wanted to do it just to acknowledge Captain Maier, who is one of your witnesses today. Thank you for allowing me to introduce him.

I have the privilege of representing part of Oakland County, Michigan, and Captain Mel Maier from Oakland County Sheriff's Office, he commands the Emergency Communication and Operations Division. He has also been one of the foremost advocates for modernizing our Nation's emergency communications as chairman of the Public Safety Next Generation 9–1–1 Coalition.

Captain Maier is responsible for overseeing radio and 9–1–1 emergency communications within the sheriff's operations center and is the sheriff's communications representative within Oakland County's Homeland Security and Emergency Operations Center. He began his career in law enforcement more than 28 years ago as a patrol officer with the Garden State Police Department before joining the Oakland County Sheriff's Office in 2009. He is one of our local leaders.

I describe him, Captain Maier, as one of Michigan and the Nation's most knowledgeable experts on the subject of emergency communications and has been a, quote, stalwart champion of connecting our first responders and communities over two decades. He led the deployment of the text to 9–1–1 technology for Oakland County, and he has been at the forefront of developing shared emergency communications in Michigan.

So it is my pleasure just as the Representative of part of Oakland County to welcome him to the committee today.

Mrs. DEMINGS. Representative Slotkin, thank you so much for that introduction.

Captain Maier, thank you so much for joining us today.

Our third witness is Chris Lombard, the deputy chief of the Seattle Fire Department. Chief Lombard was a member of the first service who responded to Ground Zero in Manhattan for 2 weeks.

Chief Lombard, we thank you so much for your service on that day and your continued service to this day.

Chief Lombard has been active in the fire service for nearly 30 years, mainly with the Seattle Fire Department. In addition to 9/11, he has also responded to incidents, including the Washington landslide and hurricanes in the Pacific, Atlantic, and Gulf of Mexico.

Chief Lombard works in the Seattle Fire Department's Operation Division and 9–1–1 center, and manages communications coordination for the Department's specialty teams.

Chief Lombard, it is an honor to have you with us today, and thank you so much for joining us.

The Chair now recognizes the Ranking Member to introduce our fourth witness from the great State of Florida.

Mrs. CAMMACK. Thank you, Madam Chairwoman. I see you chuckling, because everyone has been wondering on this call, is Gator actually his name? I can report that, yes, he is named Gator.

So it is with great affection and a pleasure to introduce my friend but also one of our fantastic sheriffs in north central Florida, Sheriff Gator DeLoach. A lifelong resident of Putnam County, he has had a long career in public service, starting over 20 years ago. Sheriff DeLoach has played integral roles throughout his law enforcement career, from sergeant, where he held leadership positions in the drug unit, patrol, and property crimes, to lieutenant of Criminal Investigations Bureau.

In January 2017, Sheriff DeLoach was sworn in as sheriff of Putnam County, and we are so lucky to have you in that role. I am honored to be your Representative in Congress, and thank you for your continued service to our community, as well as your work on several of the task forces that we have. So thank you again for your testimony here today, Sheriff DeLoach. Again, yes, his name actually is Gator.

I yield back.

Mrs. DEMINGS. Thank you to the Ranking Member.

Let this Florida State Seminole welcome you, Sheriff Gator DeLoach.

Thank you so much to all of our witnesses for joining us today.

Without objection, the witnesses' full statements will be inserted in the record.

I now ask each of our witnesses to summarize their statement for 5 minutes, beginning with Dr. Rodriguez.

**STATEMENT OF CHRISTOPHER RODRIGUEZ, DIRECTOR, HOMELAND SECURITY AND EMERGENCY MANAGEMENT AGENCY, DISTRICT OF COLUMBIA**

Mr. RODRIGUEZ. Thank you.

Good afternoon, everyone, Chairwoman Demings, Ranking Member Cammack, Members of the subcommittee, and especially greetings to our New Jersey Representatives, Bonnie Watson Coleman and Donald Payne, who I worked very closely with when I was the State director in 2014 and 2017.

My name is Dr. Christopher Rodriguez. I am the director of the D.C. Homeland Security and Emergency Management Agency. As an appointee of D.C. Mayor Muriel Bowser, I am honored to be before this committee to talk about the strides that the District of Columbia has made in emergency communications since the tragic events of 9/11.

When it comes to emergency communications, there is really no place in the country and perhaps in the world like the National Capital region. With frequent special events and the ever-present threat of disasters, terrorism, the hazard landscape here in the district is unique. We are home to over 40 Federal and local response agencies, and we have a robust mutual aid system that spans the mid-Atlantic region. All of us need to communicate seamlessly and reliably across the whole spectrum of possible contingencies.

I think when people often think or talk about emergency communications, they think in terms of radios. But the solutions to these communications challenges that we now face are multifaceted, and they span technologies beyond just land mobile radios. With my time today, I would just like to discuss a few key solutions, successes, and challenges that are unique to the District.

As mobile data and cellular communications become increasingly important elements of effective emergency response, the District first utilized FirstNet for first responders in 2018. By providing dedicated cellular connectivity for the public safety community, FirstNet enables us to continue sharing voice data and video even in the face of extreme network congestion.

Additionally, our partnership with FirstNet has enabled us to request rapidly deployable cellular infrastructure to support the demands of large events and incidents.

Leading up to the 2021 Presidential inauguration and on January 6, we had coordinated with FirstNet to have such infrastructure in place to cover the U.S. Capitol complex. Ultimately, this collaboration and their dedicated bandwidth allowed FirstNet to perform reliably for our first responders at the U.S. Capitol on January 6.

We are now in the process of working with FirstNet to acquire two of our own compact rapid deployable units, which will contribute to increased resilience and self-sufficiency for the District's emergency communications.

While the ability to communicate between Government partners is vital, the ability to quickly reach the public with life-saving information is equally important. There are many ways to quickly push emergency information to the public during a crisis, but a unique challenge to the District is that we receive an extremely high volume of visitors and transient populations. These individuals may not be in the District long enough to sort-of learn about our opt-in emergency notification systems or follow our public safety officials on social media.

Wireless Emergency Alert, or WEA, has proven to be an incredibly valuable resource in our public learning and warning toolbox. My agency has been both a regional and National leader in the WEA space since it was tested before the 2017 Presidential inauguration.

Following the successful first test, which was the first of its kind in the Nation, our staff were asked to share best practices on alerting procedures with our State, local, Tribal, territorial, and even FEMA partners.

But while WEA is a powerful tool, it is not without its limitations. We still see challenges with the accuracy of geofencing, which can lead to bleed over outside of our intended target area. It is also a very high-profile alerting method and its overuse or inappropriate use can lead individuals to opt out of the service, which would limit our ability to reach them in a dire emergency. We did use WEA in announcing curfews during the Black Lives Matter protests and the January 6 insurrection, as well as with other extreme weather events.

So improving the interoperability and reliability of emergency communications here in the District is a top priority for us and I know for the Mayor. I appreciate the opportunity to share these experiences with the subcommittee, so thank you very much.

[The prepared statement of Dr. Rodriguez follows:]

PREPARED STATEMENT OF CHRISTOPHER RODRIGUEZ

OCTOBER 7, 2021

Thank you, Chairwoman Demings, Ranking Member Cammack, and Members of the subcommittee. My name is Dr. Christopher Rodriguez and I am the director of the DC Homeland Security and Emergency Management Agency. As an appointee of Mayor Muriel Bowser, I am honored to lead an agency that is a National leader in emergency management. I appear today to speak with you about the strides the District of Columbia has made in emergency communications since the tragic events on 9/11.

When it comes to emergency communications, there is no place like the National Capital Region. With frequent special events and the ever-present threat of terrorism and disasters, the hazard landscape in the District of Columbia is unique. The District is home to over 40 local and Federal response agencies, and we have a robust mutual aid system that spans the Mid-Atlantic region. All need to communicate seamlessly and reliably across the whole spectrum of possible contingencies.

People often think of emergency communications solely in terms of radios. But the solutions to these communications challenges are multifaceted and span technologies beyond just land mobile radios. With my time today I will discuss a few key solutions, successes, and challenges that are unique to the District.

As mobile data and cellular communications become increasingly important elements of effective emergency response, the District first utilized the FirstNet service for our first responders in 2018. By providing dedicated cellular connectivity for the public safety community, FirstNet enables us to continue sharing voice, data, and video even in the face of extreme network congestion. Additionally, our partnership with FirstNet has enabled us to request rapidly deployable cellular infrastructure to support the demands of large events and incidents. Leading up to the 2021 Presidential Inauguration and on January 6, we had coordinated with FirstNet to have such infrastructure in place to cover the U.S. Capitol complex. Ultimately, this collaboration and their dedicated bandwidth allowed FirstNet to perform reliably for our first responders at the U.S. Capitol on January 6. We are in the process of working with FirstNet to acquire two of our own compact rapid deployable units, which will contribute to increased resilience and self-sufficiency for the District's emergency communications.

While the ability to communicate between government partners is vital, the ability to quickly reach the public with life-saving information in emergency situations is equally important. There are many ways to quickly push emergency information to the public during a crisis, but a unique challenge in the District is that we receive an extremely high volume of visitors and transient populations. These individuals may not be in the District long enough to learn about opt-in emergency notification systems or follow public safety officials on social media. Wireless Emergency Alert, or WEA, technology has proven to be an incredibly valuable resource in our public alert and warning toolbox.

The DC Homeland Security and Emergency Management Agency has been both a regional and National leader in the WEA space since just before the 2017 Presidential Inauguration, when we became the first local alerting authority to issue a live WEA test. Following this successful test, our staff were asked to share best practices and alerting procedures with State, local, Tribal, territorial, and even our FEMA partners. While WEA is a powerful tool, it is not without limitations. The accuracy of geofencing is not perfectly accurate, which can lead to bleed over outside of the intended target area. Additionally, WEA is a high-profile alerting method. Overuse or inappropriate use of the technology can lead to individuals opting out of the service which would limit or ability to reach them in a truly dire emergency. The District has found success in using WEA for situations such as Boil Water Advisories, announcing curfews (for example during the BLM protests), and extreme weather events. While WEA remains an incredibly effective tool to alert the public in the District, we employ a multi-modal approach which includes our Opt-In Alert DC program, Integrated Public Alert & Warning System (which includes WEA), social media and traditional media messaging, and door-to-door canvassing.

Improving the interoperability and reliability of emergency communications systems is a top priority for the District of Columbia. I appreciate the opportunity to share our experiences with the subcommittee.

Thank you, and I look forward to your questions.

Mrs. DEMINGS. Thank you so much, Dr. Rodriguez, for your testimony.

I now recognize Captain Maier to summarize his statement for 5 minutes.

## STATEMENT OF MEL MAIER, CAPTAIN, OAKLAND COUNTY SHERIFF'S OFFICE

Mr. MAIER. Good afternoon, Chairwoman Demings, Ranking Member Cammack, and thank you to Congresswoman Slotkin for that introduction, and Members of the subcommittee. I am Mel Maier, a captain in the Oakland County, Michigan, Sheriff's Office.

The sheriff of Oakland County, Michael J. Bouchard, is a member of the Major County Sheriffs of America, MCSA, and I offer my comments today on behalf of all their members represented by that association.

I will spend a minute each on four issues: Radio communications interoperability, 9–1–1 systems, FirstNet, and IPAWS. I look forward to your questions afterwards.

Overall, 20 years after the 9/11 attacks, we have made a lot of progress in emergency communications, but there is still more to be done. We need to meet the needs and expectations of the American people in the 21st Century.

The ability to communicate and coordinate via radio networks is essential, no matter the type of incident we are responding to, whether it is a highway crash, an active shooter, a wildfire, hurricane, or terrorist attack. Since 9/11, more advanced radio features and technologies have improved interoperability between public safety agencies.

Funding from the Department of Homeland Security's UASI and State Homeland Security grant programs has helped us improve infrastructure and get responder devices into the field. However, barriers to radio communications technology growth and intraoperability still exist. There still remains at times lack of coordination and intraoperability among agency communications systems due to the varying levels of radio technology, system maturity, and continued reliance upon legacy proprietary systems.

Additional Federal funding would help us accelerate the move to modern systems and true intraoperability. It would help agencies implement technologies that can bridge those different communication networks, enabling data and voice intraoperability.

Regarding 9–1–1, we are on the verge of seeing Next Generation 9–1–1 become much more widely deployed across the United States. Next Generation 9–1–1 was developed to address longstanding issues with legacy 9–1–1 systems. This technology [inaudible] like FirstNet. However, without Federal funding, many jurisdictions will not be able to transition to NG 9–1–1 any time soon. This will create a patchwork of haves and have-nots, resulting in uneven capabilities throughout the United States, and that is not fair to the responders or to the citizens. Some 9–1–1 centers will achieve NG 9–1–1, while others, especially those in rural areas, will not have the means.

The Public Safety Next Generation 9–1–1 Coalition includes many of the leading organizations in the country representing fire, EMS, law enforcement, and emergency communications professionals. We are advocating for a one-time commitment of $15 billion in Federal grant funding to support a Nation-wide transition to NG 9–1–1.

MCSA strongly believes this once-in-a-generation investment will allow the successful deployment of NG 9–1–1 Nation-wide. It improves emergency response. It saves lives.

With regards to FirstNet, the 9/11 Commission recommended establishing an interoperable Nation-wide broadband network dedicated solely to first responders. Through this leadership of the public safety community and Congress, we now have FirstNet, a reli-

able, dedicated, Nation-wide high-speed network solely for first responders.

Since FirstNet's creation, coverage and capacity have consistently improved. There is a dedicated network core that is completely focused on public safety. There are now over 2.5 million FirstNet connections across 17,000 public safety agencies and other organizations, and the FirstNet Authority is looking further ahead toward 5G connectivity for public safety in its course dedicated core.

At the same time, the success of FirstNet ultimately depends on continued investment in the development of reliable coverage and capacity throughout the United States. The network's roll-out has been fast by any standard, and there is still progress to be made. Congress should continue to ensure that FirstNet Authority gets the support it needs to realize the full promise of FirstNet.

Finally, with regard to IPAWS, FEMA has simplified the system, improved the ability to quickly reach more in the public. In my home State of Michigan, during the COVID pandemic, we utilized IPAWS to provide information on public health orders and other recommendations, which resulted in successfully messaging the important public health emergency information.

At the same time, there are opportunities to upgrade the system. Current IPAWS systems do not work on older cellular devices and may fail to reach the targeted public. Geofencing is an inaccuracy, as you heard the previous speaker state. IPAWS should continue to better integrate and leverage IP-based systems, including integration of NextGen 9–1–1.

I want to thank you, Chairman Demings and Ranking Member Cammack, for focusing on this critically important issue. Every single one of our citizens deserves to have their first responders equipped with the best and most reliable emergency communications systems. I look forward to your questions.

[The prepared statement of Mr. Maier follows:]

PREPARED STATEMENT OF MEL MAIER

OCTOBER 7, 2021

INTRODUCTION

Good afternoon Chairwoman Demings, Ranking Member Cammack, and Members of the subcommittee. I am Mel Maier, a captain in the Oakland County, Michigan Sheriffs Office. Currently, I am the commander of the Emergency Communications & Operations Division. As commander, I am responsible for overseeing our radio and 9–1–1 emergency communications and manage our Operations Center. I have been a sworn law enforcement officer for more than 31 years and have significant experience with and insight into emergency communications technology and policy challenges.

I am pleased to testify before your subcommittee to discuss the current state of emergency communications. I intend to offer my own first-hand knowledge of the current state of emergency communications and considerations for future progress. The sheriff of Oakland County, Michael J. Bouchard, is a member of the Major County Sheriffs of America (MCSA) and I offer my comments today on behalf of other members represented by that Association. Truly, the issues we face here in Oakland County are similar to those faced by sheriff's offices and our colleagues in public safety agencies across the country.

The tragedy of September 11, 2001 revealed fundamental problems with communication systems used by our Nation's first responders. These issues ranged from the lack of a dedicated broadband network for public safety communications to issues with interoperability and communication between radio networks and

9–1–1 systems. Twenty years later, significant progress has been made to address these shortcomings. However, much more needs to be done to meet the needs and expectations of the American people in the 21st Century. Thank you for the opportunity to share my perspective on these critical issues.

RADIO COMMUNICATIONS

Since 9/11 more advanced radio features and usage policies have improved resiliency and system capacity and led to more and better coordination between first responders. The ability to communicate and coordinate via radio networks is essential no matter the type of incident we are responding to, whether it is a highway crash, an active shooter, a wildfire, a hurricane, or a terrorist attack. APCO Project 25 standards and the P25 CAP program have improved interoperability. Specific features such as advanced trunking, dedicated event talk groups and both encrypted and clear channels for Law Enforcement, Fire, Emergency Medical Service, and Emergency Management have improved how we use the radio technology. Funding from the Department of Homeland Security's Urban Area Security Initiative Program (UASI), dedicated to interoperability, has been pivotal in providing resources to improve infrastructure and field responder devices. In addition, tabletop and field-based exercises have been effective in identifying gaps between communication systems and in establishing better operational policies.

However, barriers to radio communications technology growth and interoperability still exist. Vendor solutions often introduce new features and (at times mandatory) upgrades to P25 systems that impede or defeat any interoperability gains. There is still a lack of coordination and interoperability among agency communication systems and varying levels of system maturity including the continued reliance upon legacy proprietary systems. Increasing costs and decreased Federal investments have made support for radio communications harder to maintain.

Additional Federal funding would be helpful in improving overall radio communications capabilities, and in helping agencies implement technology that can bridge different communications networks. Public safety grade networks have become increasingly popular targets for cyber attacks, and sustainment of these systems will require more on-going costs to support cybersecurity protections. Systems need to advance to be able to share voice and data to increase first responder situational awareness. We should also consider adopting standardized encryption key management features to better support interoperability among first responder agencies. Additional grant opportunities and stronger grant conditions, accountability, and compliance programs for vendors might help provide the incentives needed to improve interoperability.

9–1–1 AND NEXT GENERATION 9–1–1

Our Nation's 9–1–1 systems are critical infrastructure relied upon Nation-wide every day by citizens seeking assistance in a variety of life-or-death situations. Since 9/11, new 9–1–1 technology called Next Generation 9–1–1 (NG 9–1–1) has been developed to address long-standing issues with our legacy 9–1–1 systems. This technology offers improvements to a wide range of issues that affect emergency response times and capabilities.

Many of the 9–1–1 networks across the United States have not kept up with advances in communications technology and, in large part, are based upon technology dating back to the 1960's. Legacy 9–1–1 systems are built on old copper landline systems and Public Safety Answering Points (PSAP) are often not able to accept and process texts, images, videos and other modern data formats. Additionally, 9–1–1 systems have become popular targets of ransomware and denial-of-service cyber attacks by malign actors. These cyber events have taken entire 9–1–1 systems off-line, threatening emergency response times and risking public safety.

Jurisdictions across the Nation have begun to transition to Next Generation 9–1–1 systems to match capabilities first responders are receiving from FirstNet. NG 9–1–1 systems can acquire and integrate additional information useful to handling 9–1–1 requests, like photos, videos, and location data and support sharing information related to 9–1–1 requests for emergency assistance among emergency communications centers and emergency response providers.

However, without Federal funding, many jurisdictions will not be able to transition to this new technology. This will create a patchwork of "haves" and "have-nots" creating sub-optimal responses and uneven capabilities throughout the United States. Some 9–1–1 centers will achieve NG 9–1–1 while others, especially those in rural areas, will not have the means.

As a founding member of the Public Safety Next Generation 9–1–1 Coalition, the Major County Sheriffs of America, together with the International Association of

Chiefs of Police, International Association of Fire Chiefs, Major Cities Chiefs Association, Metropolitan Fire Chiefs Association, National Association of State EMS Officials, and National Sheriffs' Association is advocating for a one-time commitment of $15 billion in Federal grant funding to support a Nation-wide transition to NG 9–1–1. MCSA strongly believes this once in a generation investment will allow the successful deployment of NG 9–1–1 Nation-wide, improve emergency response, and save lives.

FIRST NET—NATION-WIDE PUBLIC SAFETY BROADBAND NETWORK

The 9/11 Commission Report recommended establishing an interoperable Nation-wide broadband network dedicated solely to first responders. The public safety community, encouraged by the 9/11 Commission report, worked together to advocate for Congress to pass legislation establishing a reliable, dedicated, and Nation-wide high-speed network solely for first responders. In 2012, Congress passed the Middle-Class Tax Relief and Jobs Creation Act which allocated $7 billion and 20 megahertz of broadband spectrum to establish a network for the Nation's first responders. It also established the FirstNet Authority, an independent entity, within the Department of Commerce, to ensure the build-out, operation, and maintenance of that network.

Today, public safety utilizes FirstNet to support a wide variety of emergency incidents, including hurricanes, wildfires, search-and-rescue missions, and many other small and large multi-jurisdictional responses. Since the network's creation, coverage and capacity have consistently improved. Public safety agency costs have been reduced. Deployable communications assets have been dedicated to FirstNet users across the Nation. The FirstNet Authority is looking further ahead toward 5G connectivity for public safety. It is also working to facilitate Land Mobile Radio (LMR) to LTE interfaces to provide complementary services when field responders need extended network coverage. Overall, the Nation-wide deployment of Band 14 for public safety is moving at a rapid pace.

The success of FirstNet ultimately depends on continued investment in the development of reliable coverage and capacity throughout the United States. FirstNet should continue to ensure the security of public safety data and ensure secure information exchange. FirstNet should continue to engage and consult directly with public safety and support the Public Safety Advisory Committee and look for opportunities to reduce costs to public safety. FirstNet should also continue to develop direct-mode mission-critical push-to-talk to provide first responders reliable voice communications using the network and prioritize FirstNet core development.

INTEGRATED PUBLIC ALERT & WARNING SYSTEMS

The Integrated Public Alert & Warning System (IPAWS) from FEMA has simplified the public notification system and improved the ability to quickly reach more of the public. IPAWS provides the public with information related to immediate safety issues, information related to recovery efforts, and links and direction to gain additional assistance or information. The system also supports multiple languages, which is critical when serving diverse populations. During the COVID–19 pandemic, we utilized IPAWS to provide information on health orders and recommendations, as well as testing and vaccination information. We have also utilized IPAWS to successfully engage the community on missing and wanted person alerts through Amber and Silver Alerts.

There are many opportunities to upgrade the National emergency alerting system. Current IPAWS systems do not work on older cellular devices. IPAWS should continue to better integrate and leverage IP-based systems including integration into Next Generation 9–1–1 systems, to provide messages outbound and inbound to Emergency Communications Centers over a secure and reliable network.

Thank you for the opportunity to address you today and I welcome any questions you may have.

Mrs. DEMINGS. Thank you so much, Captain Maier, for your testimony. There was a little bit of a connectivity issue there. I know that our team is going to troubleshoot with your team. So thank you so much for being with us today.

The Chair now recognizes Chief Lombard to summarize his statement for 5 minutes.

**STATEMENT OF CHRIS LOMBARD, DEPUTY CHIEF, SEATTLE FIRE DEPARTMENT, ON BEHALF OF INTERNATIONAL ASSOCIATION OF FIRE CHIEFS**

Mr. LOMBARD. Good morning, Chairwoman Demings and Ranking Member Cammack. I am Chris Lombard, the deputy fire chief with Seattle Fire Department and acting chair of the Communications Committee for the International——

[Audio interruption.]

Mr. LOMBARD. I appreciate today's opportunity to discuss the progress that has been made in emergency communications since 9/11. As a responder who assisted with efforts at Ground Zero in New York, I am keenly aware of the communications issues that faced responders on that day in 2001 and the progress made since.

SAFECOM and FirstNet are two triumphs that emerged from the 9/11 Commission Report for improving intraoperability. Federal grants have also greatly improved responder communications through funding, training, information sharing, and equipment.

As others have mentioned, the First Responder Network Authority is a Nation-wide cellular network that enables first responders to communicate within and across jurisdictions, provides redundancy to ensure network resilience, and reduces the impact of network congestion. Through FirstNet, first responders have priority and preemption on dedicated public safety spectrum. On behalf of the International Association of Fire Chiefs, I ask that Congress continue to support FirstNet.

SAFECOM is also mentioned by others, a DHS advisory group, works with stakeholders to develop better technologies and processes for the coordination of communications systems. SAFECOM trains first responders in emergency communications, coordinates grant guidance, and encourages intraoperability.

As the first vice chair of SAFECOM, I have seen its great work first-hand. On behalf of the IAFC, I ask Congress to continue to support the Cybersecurity and Infrastructure Security Agency and its support of SAFECOM.

Post-9/11, the State Homeland Security Program and Urban Area Security Initiative grants have been crucial to improving emergency communications. These grants incentivize first responders across jurisdictions to collaborate before, during, and after an incident. This coordination reduces confusion and directly saves lives. Our members have used this grant funding to improve regional radio interoperability and develop resilient communications. The IAFC urges Congress to continue to support strong funding for SHSP and UASI grants.

FEMA's Assistance to Firefighter Grants and SAFER grants are also used for equipment, training, and staffing. AFG grants are key to public safety communications, especially since 50 percent of fire departments still lack enough portable radios to equip a full shift. The SAFER grants are used to address staffing shortages faced by all manner of fire departments. The IAFC asks Congress to fully fund the AFG and SAFER grants which are critical to the fire service.

Though great progress has been made in emergency communications, there is still room for improvement. Many IAFC members are often mentioning how 9–1–1 calls from jurisdictions are being

improperly routed, resulting in significant delays. We should be able to do better in an emergency, and this highlights the need for 9–1–1 infrastructure to catch up with other commercially available technology.

The IAFC is a member of the Public Safety Next Generation 9–1–1 Coalition. The Coalition requests that Congress enact legislation funding, a $15 billion NextGen 9–1–1 package via the reconciliation package.

The availability of spectrum for public safety operations is also critically important. The 4.9 gigahertz band was set aside for public safety use after 9/11. Public safety use of 4.9 gigahertz spectrum includes hosting mission-critical broadband networks. Public safety has increasingly relied on this spectrum as new technologies become more widely-used.

Last October, the FCC issued an order to set up a system of State licenses to make 4.9 gigahertz spectrum available to commercial entities. On September 30 of this year, the FCC rescinded that order and adopted a notice to seek comment on public safety and non-public safety use of the ban. The IAFC supports the FCC's decision to rescind the framework of State licenses.

Public safety also uses 6 gigahertz spectrum to support backhaul for communication systems and radio communications in rural areas across the United States. The IAFC urges Congress to continue to monitor these FCC proceedings to protect critical public safety communications in the 6 gigahertz band.

In conclusion, public safety and emergency response are perhaps the pinnacle of team sports with no higher expectations and no higher importance for getting it right. Immediately after 9/11, we recognized our challenges were people-based. We recognized that our—likewise, the successes I and others experienced on 9/11 were also because of the people and relationships we had formed.

We wouldn't be here today without the spirit of working together and the foundations by the likes of retired police chief Harlin McEwen from Ithaca, New York, and retired fire chief and past president of the IAFC, Jeff Johnson, instrumental in launching efforts like SAFECOM, FirstNet, and others. It continues today with relationships that public safety forms, like the one between Captain Mel Maier and myself, across the country.

Facilitating and forming maintenance of these relationships may be the biggest single success that the Federal Government has done, and for that we thank you.

I thank the subcommittee for all it has done to improve public safety communications in the 20 years since 9/11. I also have got to thank my family and the support team back at the IAFC, Ryan Woodward and Ken LaSala. The IAFC looks forward to continuing the work of the subcommittee and to address the continued communications needs of public safety.

Thank you very much.

[The prepared statement of Mr. Lombard follows:]

PREPARED STATEMENT OF CHRISTOPHER LOMBARD

OCTOBER 7, 2021

Good morning, Chairwoman Demings and Ranking Member Cammack. I am Chris Lombard, deputy fire chief of the Seattle (Washington) Fire Department and

acting chair of the International Association of Fire Chiefs' (IAFC) Communications Committee. I appreciate the opportunity today to discuss the progress that has been made in emergency communications since 9/11 and how Congress and first responders can build upon this progress going forward.

The IAFC represents the leadership of over 1.1 million firefighters and emergency responders. IAFC members are the world's leading experts in firefighting, emergency medical services, terrorism response, hazardous materials (hazmat) incidents, wildland fire suppression, natural disasters, search and rescue, and public safety policy. Since 1873, the IAFC has provided a forum for its members to exchange ideas, develop best practices, participate in executive training, and discover diverse products and services available to first responders.

America's fire and emergency service is an all-hazards response force that is locally situated, staffed, trained, and equipped to respond to all types of emergencies. There are approximately 1.1 million men and women in the fire and emergency service—consisting of approximately 300,000 career firefighters and 800,000 volunteer firefighters—serving in over 30,000 fire departments around the Nation. They are trained to respond to all hazards ranging from earthquakes, hurricanes, tornadoes, and floods to acts of terrorism, hazardous materials incidents, technical rescues, fires, and medical emergencies. We usually are the first on the scene of a disaster and the last to leave.

## THE STATE OF PUBLIC SAFETY COMMUNICATIONS DURING AND SINCE 9/11

As a member of the fire service who responded to ground zero in Manhattan for 2 weeks as a member of Washington Task Force 1 with FEMA's Urban Search & Rescue system in the wake of the September 11 attacks, I am keenly aware of the challenges and issues facing public safety communications on September 11, 2001; the progress we have made since; and the work that remains to be done. During the first hours after the attacks, cell phone networks were jammed, and priority cellular access was not provided to emergency responders. Radio channels and phone lines to emergency communications centers also were jammed.

In addition, there were problems with interoperability between jurisdictions. Public safety radio systems operated on various frequencies and were not interoperable. Officials struggled to coordinate the multiagency response, and to maintain command and control of the numerous agencies and responders. Pagers and runners proved to be the most effective form of communication.

The Final Report of the National Commission on Terrorist Attacks Upon the United States (also known as "the 9/11 Commission Report") identified the need for improved interoperable communications between first responders and recommended a Nation-wide public safety wireless broadband network. In the 20 years since 9/11, Congress and the administration have worked hard to bring these recommendations into fruition.

SAFECOM and the First Responder Network Authority (FirstNet) are two triumphs that have emerged from the 9/11 Commission Report's recommendations and have substantially improved first responder communications and interoperability. FEMA preparedness grants like the State Homeland Security Program (SHSP), Urban Area Security Initiative (UASI), Staffing for Adequate Fire and Emergency Response (SAFER) and Assistance to Firefighters Grant (AFG) programs also have done a great deal to improve first responder communications through funding, training, information-sharing efforts, and equipment. I thank the committee for all it has done in the years since 9/11 to bring about these improvements.

## FIRSTNET

Interoperability involves the ability of public safety service and support providers—law enforcement, firefighters, EMS, emergency management, public utilities, transportation, and others—to communicate with staff from other responding agencies, and to exchange voice and/or data communications on demand, when authorized and in real time. To address the 9/11 Commission Report's recommendations to improve interoperability and establish a Nation-wide public safety wireless broadband network, Congress incorporated a key public safety communications provision in The Middle Class Tax Relief and Job Creation Act of 2012 (Pub. L. 112–96). This legislation provided the necessary 20 MHz of spectrum in the 700 MHz band and $7 billion to build a Nation-wide broadband network dedicated to the mission requirements of public safety. It also created the First Responder Network Authority (FirstNet), as an independent agency in the U.S. Department of Commerce.

While mentioning Pub. L. 112–96, I would like to take an opportunity to thank this subcommittee for their work to remove a provision of this bill that would have dealt a tremendous blow to public safety, the T-Band Auction mandate. This man-

date would have required the auctioning of T-Band (470 MHz—512 MHz) spectrum starting this year and would have required public safety to vacate this spectrum by 2023. The GAO report requested by Rep. Payne and former Reps. Donovan and King showed just how irreplaceable this spectrum is for the operations of public safety's land mobile radios in 11 metropolitan areas across the country, an area that covers 20 percent of the Nation's population.

Pub. L. 112–96, also authorized FirstNet to enter a public-private partnership to deploy the network. Through a competitive bidding process, FirstNet selected AT&T as its partner in March 2017. AT&T has been deploying the network as specified in its contract and in State-specific plans, with 80 percent of the network buildout completed. I personally think public-private partnerships are extremely valuable to public safety communications. Public safety has a very low turnover rate relative to the private sector, and as a result can be very slow to adopt new technologies. Public-private partnerships offer the opportunity to pair the adaptability of the private sector with the knowledge and resources of the public sector.

FirstNet became operational in March 2018 and is based on a single, National network architecture that evolves with technological advances and consists of a physically separate evolved packet core (EPC) network and radio access networks (RANs). This Nation-wide network enables first responders to communicate with one another within and across jurisdictions. FirstNet allows multiple agencies to be interoperable on-scene at an incident. It also provides redundancy which allows it to be more resilient than commercial networks and prevents the network being jammed by users during an emergency.

The FirstNet network supplements legacy voice systems by providing public safety entities with mission-critical advanced data and voice capabilities and services including, but not limited to messaging, image sharing, video streaming, group text, voice, data storage, application, location-based services, and preemption. It also provides applications, and deployable assets that can restore communications after disasters.

Agencies are subscribing to and using the network in emergencies, including the COVID–19 pandemic and wildland fires. In his testimony to the Senate Committee on Commerce, Science, and Transportation's Subcommittee on Communications, Media, and Broadband in June, Chief Jeffrey Johnson, chief executive of the IAFC's Western Division said:

"Before FirstNet, field-based first responders, such as wildland firefighters, were hesitant to adopt new technology solutions because they couldn't count on it working when they needed it most. Now that we have FirstNet, first responders have priority and preemption, dedicated 700 MHz public safety spectrum that has been built out across the country (with aggressive rural coverage build benchmarks—an important priority for the WFCA), and the ability to request portable cell towers (Colts and Cows) to make sure first responders have connectivity, such as in the event infrastructure has been damaged by a fire or when a command post is staged in a remote mountainous area."

On behalf of the IAFC, I ask that Congress continue to support FirstNet in its mission to fulfill the 9/11 Commission Report's recommendation of a Nation-wide public safety wireless broadband network.

SAFECOM

Another entity that has been critical to fulfilling the 9/11 Commission Report's recommendation of improved interoperability is SAFECOM. SAFECOM was formed in 2001 after the September 11 terrorist attacks, as part of the Presidential E-Government Initiative to improve public safety interoperability, allowing emergency responders to communicate effectively before, during, and after emergencies and disasters. SAFECOM's mission is to improve designated emergency response providers' interjurisdictional and interdisciplinary emergency communications interoperability through collaboration with emergency responders and elected officials across Federal, State, local, Tribal, and territorial governments, and international borders.

As the first vice chairman of SAFECOM, I have seen first-hand the great work it has done to fulfill its mission. SAFECOM is one of the first organizations to bring together representatives from public safety associations as well as emergency responders in the field. Its membership includes more than 60 members representing Federal, State, local, Tribal, and territorial emergency responders, and major intergovernmental and National public safety associations. I serve on SAFECOM in my capacity as deputy chief of the Seattle Fire Department. The IAFC also has two representatives to SAFECOM's membership, including Greg Rubin, assistant chief of Miami-Dade (Florida) Fire Rescue.

SAFECOM is managed by the Cybersecurity and Infrastructure Security Agency (CISA) and works with existing Federal communications programs and key emergency response stakeholders to address the need to develop better technologies and processes for the coordination of existing communications systems and future networks. SAFECOM focuses both on technology and the need for jurisdictions to develop an effective command interoperability plan. SAFECOM trains emergency responders to be communications unit leaders during all-hazards emergency operations, and coordinates grant guidance to use Federal funding to encourage interoperability.

Through their partnerships, SAFECOM has created key documents such as the Interoperability Continuum, the Statement of Requirements (SoR) for baseline communications and interoperability standards, the State-wide Communication Interoperability Plan (SCIP) Methodology, and the National Emergency Communications Plan (NECP) to assist emergency responders Nation-wide with improving communications and interoperability.

SAFECOM serves as a tremendous resource to first responders in providing key guidance to attain grant funding, improve interagency communications, and develop interjurisdictional and interagency relationships. On the behalf of the IAFC, I ask Congress to continue support CISA in its management of SAFECOM.

THE NEED FOR INVESTMENT IN NEXT GENERATION 9–1–1 (NG 9–1–1)

Public safety fought hard to establish FirstNet because we knew that we were being left behind compared to the technologies available for personal-use communications. The same holds true for NG 9–1–1. First responders handle over 240 million emergency 9–1–1 calls per year. Unfortunately, 9–1–1 networks across the United States have not kept up with advances in communications technology and, in large part, are based upon technology dating back to the 1960's.

Even though 9–1–1 systems are critical infrastructure in every community, they are underfunded and technologically inadequate to address the needs and expectations of the American people in the 21st Century. While 9–1–1 operations are State and local functions, the investment of Federal resources in this critical infrastructure will ensure that all communities in the United States will have a secure, resilient, interoperable, and reliable way of receiving, processing, and responding to requests for emergency assistance.

IAFC member and Philadelphia Fire Commissioner, Adam Thiel equates the upgrading of our Nation's 9–1–1 infrastructure to NG 9–1–1 to shifting from a rotary phone to a smart phone. When discussing issues concerning the current state of 9–1–1 infrastructure, Commissioner Thiel often speaks about how 9–1–1 calls coming from his jurisdiction in Philadelphia are often routed across the river to Camden, New Jersey. This results in significant delays due to having the call re-routed to the 9–1–1 center in Philadelphia. IAFC members around the country have spoken of similar issues and delays. This is unacceptable in an emergency situation where every second counts.

The focus on improving our Nation's infrastructure provides a unique opportunity for Congress to make a once-in-a-generation investment to modernize our 9–1–1 systems to NG 9–1–1. NG 9–1–1 will enable Emergency Communications Centers (ECCs) to receive a variety of multimedia (photos, videos) and other data from 9–1–1 callers and seamlessly share this information with other ECCs and responding fire, EMS, and law enforcement officials in the field. This will make emergency responses faster and more efficient and make public safety professionals and the communities they serve safer. Simply put, NG 9–1–1 will save lives.

The IAFC is a member of the Public Safety Next Generation 9–1–1 Coalition, which consists of the Metropolitan Fire Chiefs Association, the Major County Sheriffs of America, the Major Cities Chiefs Association, the National Association of State EMS Officials, the National Sheriffs' Association, the International Association of Chiefs of Police, and the Association of Public-Safety Communications Officials International. This coalition is advocating for a one-time $15 billion NG 9–1–1 upgrade to be part of the reconciliation package Congress is currently considering.

A 2018 study requested by Congress and conducted by the National Highway Traffic Safety Administration determined that $9.5–12.7 billion was required to achieve NG 9–1–1 Nation-wide. In the time since this study was completed, our 9–1–1 infrastructure has faced additional challenges like increased cybersecurity threats. To adequately meet these challenges and cybersecurity concerns, $15 billion is needed to upgrade our Nation's 9–1–1 infrastructure most effectively.

Additionally, the IAFC and the Public Safety Next Generation 9–1–1 Coalition are requesting that the following NG 9–1–1-related priorities be included in the reconciliation package along with $15 billion in funding for the NG 9–1–1 upgrade:

(1) Ensure that NG 9–1–1 is interoperable by requiring the use of standards that are commonplace in the consumer marketplace.

(2) Funding for training, so that an on-scene incident commander can properly prioritize the data they receive.

(3) Establish a Next Generation 9–1–1 Advisory Board to ensure NG 9–1–1 grants meet the needs of public safety professionals and the public they serve.

(4) Establish a Nation-wide Next Generation 9–1–1 Security Operations Center to meet the vital 9–1–1-related cybersecurity needs of local public safety agencies.

All the priorities listed above are in the House's reconciliation proposal (H.R. 5376). H.R. 5376 only provides $10 billion in funding for NG 9–1–1. The IAFC and Public Safety NG 9–1–1 Coalition hope the Senate will include our NG 9–1–1 priorities in their reconciliation proposal along with $15 billion in funding, and that the House will support this funding as well.

IMPORTANCE OF SHSP AND UASI GRANTS

The SHSP grants assist State, local, Tribal, and territorial efforts to build, sustain, and deliver the capabilities necessary to prevent, prepare for, protect against, and respond to acts of terrorism. The UASI program assists high-threat, high-density urban areas' efforts to build, sustain, and deliver the capabilities necessary to prevent, prepare for, protect against, and respond to acts of terrorism. In the wake of the terrorist attacks on 9/11, both grant programs have been crucial in assisting public safety to be better prepared and trained to address a terror attack or any major incident that may occur in their communities.

The great success of SHSP and UASI is that they provide an incentive for Federal, Tribal, State, territorial, and local jurisdictions to collaborate before, during, and after an incident. By planning, training, and conducting exercises together, local fire chiefs, police chiefs, sheriffs, public health officials, emergency managers, and State and Federal officials are prepared to work together in the event of an emergency. This preplanning and coordination prevent confusion during an incident and directly saves lives.

The IAFC's members and the communities they serve have strongly benefited from SHSP and UASI grant funding. Many of our members have utilized this funding to strengthen their information sharing and communications abilities. Our members in the National Capitol Region (NCR) have utilized funding from these programs to develop several emergency communications functions to aid in providing information during an emergency. Through these systems, residents in every jurisdiction throughout the NCR can sign up for free text messaging alert systems from local governments that provide real-time emergency alerts and notifications to cell phones, pagers, email accounts.

The NCR has also utilized this funding to interconnect the fiber optic networks built and funded by the local jurisdictions to form the "NCR Net." This system enables the seamless transmission of critical data such as that used by computer-aided dispatch systems throughout the region thus elevating situational awareness and reducing emergency call processing time. IAFC members in California have utilized this funding to improve regional radio interoperability, develop resilient internal communications, improve fire station security, and train chiefs and company officers to lead in large-scale and complex incidents.

IAFC members in Clark County Nevada have used these funds to support fusion center activities within the Southern Nevada Counterterrorism Center. These activities include suspicious activity analysis and reporting; evaluation and support of special events; multi-agency intelligence and information sharing; and the hardware and software to support these programs. They also have utilized this funding to support community outreach and education programs like "See Something, Say Something" campaigns; training and exercises; and the development of public/private partnerships to help protect the region.

The IAFC is pleased that the Department of Homeland Security Appropriations Act, 2022 (H.R. 4431) contains $705 million for UASI and $610 million for SHSP. We urge Congress to continue to support strong funding for these important grant programs.

IMPORTANCE OF AFG AND SAFER GRANTS

The AFG and SAFER grant programs are critical to the fire and EMS service. The AFG program is one of the few grant programs dedicated to all-hazards prepared-

ness and response. The AFG grant program was created in 2000 as part of the Fiscal Year 2001 National Defense Authorization Act (Pub. L. 106–398) to improve the baseline operational capability of America's fire service through improved equipment, training, and staffing.

The SAFER grant program was created in 2003 as part of the fiscal year 2004 National Defense Authorization Act (Pub. L. 108–136) to specifically address the staffing shortages in career, volunteer, and combination fire departments. SAFER grants are especially important in today's environment where volunteer fire recruitment and retention are suffering.

AFG grants are helpful in improving public safety communications by enabling fire departments to purchase much-needed radios and communications equipment. The National Fire Protection Association's Fourth Needs Assessment of the U.S. Fire Service showed that 50 percent of all departments still do not have enough portable radios to equip all emergency responders on a shift.

The IAFC is grateful for the extra $200 million provided to each the AFG and SAFER programs during the COVID–19 pandemic and ask that Congress fully fund these programs.

### 4.9 GHZ SPECTRUM

In 2002, the Federal Communications Commission (FCC) designated the 4.9 GHz spectrum for public safety operations. This spectrum is used by public safety mostly for fixed point-to-point and secure Wi-Fi operations. Other public safety uses of 4.9 GHz spectrum include hosting broadband intranet networks, video camera networks, in-building communications, bomb disposal robot operations, and airborne public safety video operations. Public safety has increasingly relied upon 4.9 GHz spectrum as new technologies emerge and become more widely used. In a 2018 filing with the FCC, the National Public Safety Telecommunications Council reported that the number of fixed point-to-point sites on the 4.9 GHz band increased by 31 percent between 2015 and 2018.

In recent years, National public safety organizations, like the IAFC, and the FCC have disagreed about public safety's level of usage of 4.9 GHz spectrum. The FCC under Chairman Pai believed that public safety was not adequately using the 4.9 GHz band. Public safety contended that the FCC was not adequately accounting and tracking 4.9 GHz licenses. Seattle has both a single area-license and 58 licensed hops of 4.9 GHz. Seattle uses the 4.9 GHz spectrum primarily for communications backhaul to support data network connectivity as well as voice services. The network also supports the Seattle Police Department's mobile command center and is deployed on Seattle Fire Department fire boats.

Citing lack of utilization, the FCC moved to open 4.9 GHz spectrum to commercial users. Last October, the FCC issued an order adopting a State-by-State leasing framework that would have set up a patchwork regulation of State-run auctions of 4.9 GHz spectrum to commercial entities. The IAFC and multiple public safety organizations submitted comments and petitions opposing this move. After public safety organizations filed petitions for reconsideration of the FCC's order, the FCC placed a stay on last October's order in May and on September 30 the FCC unanimously rescinded the State-by-State leasing rules, finding that they risked fragmenting the band. The FCC also partially lifted a freeze on applications in this band to allow existing public safety licensees to modify their licenses and to license new permanent fixed sites.

Additionally, on September 30 the FCC adopted a Further Notice of Proposed Rulemaking that explores options to ensure public safety use of the band, including protecting public safety users from harmful interference, collecting more granular licensing data, and adopting technical standards to promote interoperability. The Further Notice also seeks comment on ways to encourage use of new technologies, including 5G, and dynamic spectrum access systems to facilitate coexistence between public safety and non-public safety uses of the band.

The IAFC is pleased with FCC's decision to rescind the State-by-State auction framework and views it as a step in the right direction. The IAFC will remain engaged with the Notice of Proposed Rulemaking regarding 4.9 GHz spectrum that was approved by the FCC on September 30 and urges Congress to monitor these proceedings to ensure public safety interests on the 4.9 GHz band are preserved.

### 6 GHZ SPECTRUM

Public safety uses 6 GHz spectrum to support backhaul for communications systems and radio communications in rural areas across the United States. This spectrum is heavily utilized by public safety with approximately 30,000 active licenses. In April 2020 the FCC voted to allow unlicensed users to operate on the 6 GHz spec-

trum. As a part of this rule, incumbents and new entrants in the 6 GHz band have established a multi-stakeholder group (MSG) to discuss concerns and find mutually-agreeable solutions to sharing the spectrum. The IAFC is a member of the MSG. The MSG continues to operate three focus groups to address issues of particular concern relating to the FCC's vote on 6 GHz band. The IAFC is a member of focus group on Harmful Interference.

The IAFC has filed comments with the FCC, critical of its move to open the 6 GHz spectrum to unlicensed users. In February IAFC, Utilities Technology Council (UTC), and other organizations submitted comments to the FCC opposing a January Public Notice opening the 6 GHz band to unlicensed client-to-client operations. The IAFC opposes this proposal because it would exponentially increase the potential for interference to licensed 6 GHz microwave systems and would make it more difficult to resolve interference complaints. The IAFC, UTC, and others followed up with reply comments in March.

The IAFC supported the inclusion of language in Pub. L. 116–20 directing the FCC to provide a report to Congress within 90 days on its progress in ensuring rigorous testing related to unlicensed use of the 6 GHz band. The IAFC continues to monitor the FCC's proceedings related to 6 GHz spectrum. The IAFC also urges Congress to monitor these proceedings to ensure public safety interests on the 6 GHz band are preserved.

CONCLUSION

I thank you for the opportunity to address the subcommittee on the landscape of public safety communications in the 20 years since 9/11. Through FirstNet, SAFECOM and strong funding for SHSP, UASI, AFG, and SAFER grants, we have come a long way in 20 years. However, there is still work to be done to protect these efforts and grants, along with ensuring full implementation of NG 9–1–1 and the protection of public safety spectrum. I thank the subcommittee for all it has done to bring about the progress that has been made in public safety communications in the years since 9/11. The IAFC looks forward to continuing to work with the subcommittee to address the continued communications needs of public safety.

Mrs. DEMINGS. Thank you so much, Chief Lombard, for your testimony.

The Chair now recognizes the sheriff from Putnam County, Sheriff DeLoach, to summarize his statement for 5 minutes.

Thank you, Sheriff, for being with us today.

## STATEMENT OF H.D. "GATOR" DELOACH, III, SHERIFF, PUTNAM COUNTY SHERIFF'S OFFICE

Mr. DELOACH. Thank you.

Members of the subcommittee, Chairwoman Demings, and Ranking Member Cammack, thank you for the opportunity to testify before this committee today.

As a sheriff in a rural Florida county, my office faces unique challenges to communicate with our emergency service providers in the field. It is my pleasure to be with you here today and to share some of the obstacles we face while we work together to ensure our Nation is best equipped to respond to emergent threats and life-safety issues alike.

I want to begin by talking about emergency communications post-9/11 to offer a rural perspective to Members of the subcommittee. Although our Nation has seen significant changes to the way that first responders communicate, there are still significant gaps and lapses in coverage areas.

Just for a little background, Putnam County is part of rural northeast Florida, situated approximately 60 miles south of Jacksonville and north of Daytona Beach. Our community and county is approximately 827 square miles, with a population near 75,000 residents. Putnam County is comprised primarily of farmland and large stands of pine forest harvested for timber. The county is fis-

cally constrained and is designated as a county of critical economic concern by the Florida legislature. This presents significant challenges to our first responders, not the least of which is our emergency communications systems.

While emergency services in rural areas look significantly different than it does for our urban counterparts, many things we do look the same. We all apply the same statutes and are held to the same standards by certifying bodies and have similar missions. What does contrast starkly, however, is how we communicate.

The majority of our Federal, State, and local partners use digital P25-based land mobile radio systems. Putnam County is an outlier in that we currently use an antiquated radio system which is based on technology developed during the second World War. Our current communications platform is an analog VHF radio system, primarily assembled with parts from decommissioned systems that were donated from other areas and were otherwise destined for a landfill. This effectively isolates us with no ability to communicate with our counterparts that we frequently work with or rely on for assistance.

Imagine a law enforcement officer and a paramedic who were responding to a domestic violence call in a rural area 25 to 30 minutes away from your current location. When you arrive, you speak to the victim who is conscious but not ambulatory and has a large laceration above the eye. Based on her description of her injuries, you suspect she may have internal injuries as well. The suspect ran into a densely forested area behind the residence. You try to reach the emergency communications center through your portable radio to request an expedited response from EMS and your backup but get no response. You then attempt to use your cell phone to call but have no luck.

Frustrated, you have no choice but to leave the victim in a vulnerable position while you return to your patrol car to use your more powerful mobile radio. The dispatchers can hear you, but your transmission is filled with static and unintelligible at times. Fortunately, the dispatcher has the foresight to send another deputy to assist, but, unfortunately, another 20 minutes will lapse before rescue arrives. The victim's condition deteriorates quickly because of the time delay. She suffers a stroke and loses her ability to speak and testify against her attacker.

In 2013, the FCC issued a mandate that required analog VHF systems to narrowband or otherwise decrease their wavelength from 25 kilohertz to 12.5 kilohertz to free up additional frequencies. The net effect of that on us here was a greatly reduced ability to transmit or receive radio traffic, especially in buildings or in isolated areas.

Post-9/11 funding was robust immediately following the attacks but seems to have waned significantly. For rural communities, this funding was significant in assisting emergency communications in receiving vital technology in a timely manner. Larger communities have funded their communications updates through their ability to leverage money from an extensive and diverse socioeconomic population. Rural communities, unfortunately, lack that advantage.

The majority of residents in communities like Putnam are older, rely on fixed incomes, and do not have diversity of economic growth

as seen in areas such as St. Johns or Orange counties. At the same time, communities such as Putnam are not so economically stagnant that we receive an overabundance of grant funding. Quite simply, we and other communities similar to ours are in a financial stranglehold where we have to choose to have the emergency responders to meet the needs of the community but have the potential to lose signal with communications, or pay to update the technology and communications but not have the people to respond to the emergency call.

Currently in Putnam County, we are still operating on the Florida Interoperability Network rather than the more up-to-date digital mutual aid model our area counterparts use. FIN is the technology developed that allows public safely counterparts to patch channels together, effectively creating a bridge that allows radio traffic and data to flow both directions.

In the immediate post-9/11 years, there was a significant emphasis on interoperability which led to the development of it. Focus on maintaining the system and others like it has all but grinded to a halt based on the use of digital mutual aid channels, which has contributed to a lack of maintenance and failure of user agencies to remain proficient in the operation of it. Furthermore, it has limitations, the most obvious of which being the users' inability to roam outside of their agency coverage area.

From our perspective, the most logical and cost-effective strategy for rural areas is regional communications systems with independent dispatch centers. Multiple users are counties which hear these systems within a geographic area and would enable the users to roam freely within their coverage area, which reduces cost based on shared infrastructure, while still maintaining the autonomy of independent dispatch centers.

Regional center models are not new. There are several well-established communication centers built Nation-wide and in Florida. These systems create additional efficiencies, the most notable of which creates a workaround allowing certain transmitters to be optimized for additional coverage, which isn't currently allowed because the FCC mandates transmitters cannot transmit more than 5 miles outside of their intended coverage area. This also can reduce the need to build costly tower sites by leveraging optimized antenna placement versus the need to build additional sites when transmitters can be tuned accordingly.

Although I am not aware of any current agreements, we do also have the ability to use existing infrastructure through partnering with internet service providers which allows for a leasing of tower space for last-mile efforts to further——

Mrs. DEMINGS. Sheriff DeLoach, excuse me, but your time has expired a couple of minutes ago. But during the line of questioning from the Members, if there is something that is still in your opening statement that you want to share with us, please seize that opportunity to do that.

[The prepared statement of Mr. DeLoach follows:]

PREPARED STATEMENT OF H.D. "GATOR" DELOACH, III

THURSDAY, OCTOBER 7, 2021

INTRODUCTION

Chairwoman Demings and Ranking Member Cammack, thank you for the opportunity to testify before this committee today. As sheriff in a rural Florida county, my office faces unique challenges to communicate with our emergency service providers in the field. It is my pleasure to be here with you today and share some of the obstacles we face while we work together to ensure our Nation is best equipped to respond to emergent threats and life safety issues.

EMERGENCY COMMUNICATIONS POST-9/11: A RURAL PERSPECTIVE

Although our Nation has seen significant changes to the way first responders communicate, there are still significant gaps and lapses in coverage areas.

*Background*.—Putnam County is part of rural northeast Florida situated approximately 60 miles south of Jacksonville and North of Daytona Beach. Our county is approximately 827 square miles with a population near 75,000 residents. Putnam County is comprised primarily of farmland and large stands of pine forest harvested for timber. The county is fiscally constrained and designated as a county of critical economic concern by the Florida Legislature. This presents significant challenges to our first responders; not the least of which is emergency communications.

While emergency services in rural areas looks significantly different than it does for our urban counterparts, many things we do look the same. We all apply the same statutes, are held to the same standards by certifying bodies and have similar missions.

What does contrast starkly is how we communicate. The majority of our Federal, State, and local partners use digital P25-based land mobile radio systems. Putnam County is an outlier, in that we currently use an antiquated radio system based on technology developed during World War II. Our current communications platform is an analog VHF radio system primarily assembled from parts of decommissioned systems that were donated from other areas and were otherwise destined for a landfill. This effectively isolates us with no ability to communicate with our counterparts that we frequently work with or rely on for assistance.

Imagine a law enforcement officer and paramedic crew responding to a domestic violence call in a rural area 25 to 30 minutes away from your current location. When you arrive, you speak to the victim who is conscious but not ambulatory and has a large laceration above their eye. Based on her description of her injuries, you suspect she may have internal injuries as well. The suspect ran into a densely forested area behind the residence. You try to reach the emergency communications center from your portable radio to request an expedited response from EMS and back-up, but get no response. You then attempt to use your cell phone to call, but no luck. Frustrated, you have no choice but to leave the victim in a vulnerable position while you return to your patrol car to use the more powerful mobile radio. The dispatchers can hear you, but your transmission is filled with static and unintelligible. Fortunately, the dispatcher has the foresight to send another deputy to assist, but unfortunately another 20 minutes will elapse before rescue arrives. The victim's condition deteriorates quickly because of the time delay, suffers a stroke and loses her ability to speak and testify against her attacker.

In 2013 the FCC issued a mandate that required analog VHF systems to narrowband or decrease their wavelength from 25 KHZ to 12.5 KHZ to free up additional frequencies. The net effect of that was a greatly reduced ability to transmit or receive radio traffic, especially in buildings or isolated rural areas.

Post-9/11 funding was robust immediately following the attacks, but has waned significantly. For rural communities this funding was significant in assisting emergency communications in receiving vital technology in a timely manner. Larger communities have funded their communications upgrades through their ability to leverage money from an extensive and diverse socio-economic population. Rural communities lack that advantage. The majority of residents in communities like Putnam are older, rely on fixed incomes and do not have the diversity of economic growth seen in areas such as St. Johns or Orange counties. At the same time communities such as Putnam are not so economically stagnant that we receive an overabundance of grant funding. Quite simply we, and other communities similar to ours, are in a financial stranglehold where we have to choose to have the emergency responders to meet the needs of the community, but have the potential to lose signal with communications or pay to update the technology in communications but not have the people to respond to the emergency call.

Currently in Putnam County we are still operating on the Florida interoperability network (FIN) rather than the more up-to-date digital mutual aid model our area counter parts use. FIN is a technology developed that allows public safety partners to patch channels together, effectively creating a bridge that allows radio traffic and data to flow both directions. In the immediate post-9/11 years there was significant emphasis on interoperability which led to development of the FIN. Focus on maintaining this system and others like it has all but grinded to a halt based on use of digital mutual aid channels which has contributed to a lack of maintenance and failure of user agencies to remain proficient in the operation of FIN. Furthermore, FIN use has limitations, the most obvious being user's inability to roam outside of their agency coverage area.

WHERE DO WE GO FROM HERE?

The logical and most cost-effective strategy for rural areas is regional communications systems with independent dispatch centers. Multiple users or counties would share these systems within a geographic area and would enable users to roam freely within the coverage area, which reduces cost based on shared infrastructure while still maintaining the autonomy of independent dispatch centers. Regional communications models are not new—there are several well-established regional communications systems built Nation-wide and in Florida. These systems create additional efficiencies; the most notable of which creates a work-around allowing certain transmitters to be optimized for additional coverage, which isn't currently allowed because the FCC mandates transmitters cannot transmit more than 5 miles outside their intended coverage area. This also can reduce a need to build costly tower sites by leveraging optimized antenna placement versus a need to build additional sites, when transmitters can be tuned accordingly.

Although I am not aware of any current agreements, we do have the ability to use existing infrastructure through internet service provider partnerships which allow leasing of tower space for last-mile efforts to further reduce cost, where feasible. This has the obvious benefit of potentially providing internet service for rural areas not previously afforded access.

CONCLUSION

While tremendous progress toward connectivity was made in the two decades since the 9/11 attacks, there still remains a significant amount of work to bridge the communications interoperability gap. In summary, if we are unable to talk and receive messages, we are unable to help those in need during their most critical time.

Mrs. DEMINGS. We want to thank you so much for joining us today. Matter of fact, I want to thank all of our witnesses for your testimony.

I would remind the subcommittee that we will each have 5 minutes to question the panel.

I will now recognize myself for questions.

I want to start with Chief Lombard. You said having been on the ground during 9/11, you said something to the effect of you are, of course, keenly aware of the conditions on the ground that day. We know one of the major challenges was intraoperability. Could you just kind-of talk a little bit more what it was like on the ground that day? Then, since 9/11, paint a picture for us of the improvements that we have made but we still need to make.

Thank you.

Mr. LOMBARD. Sure, Chair. Thank you very much for the question. So I responded with—so the FEMA contracts around the Nation to form 28 Urban Search and Rescue teams. The Seattle Fire Department is part of one of those teams, so we responded. We were actually in what was the second round, and it was definitely a life-altering experience. The sights, the sounds, the smells, like nothing I have ever seen since or had never seen before. Like you, I was coming off duty that morning and saw the news on the TV, and it was, again, life-altering.

When we responded to New York, one of the challenges is that even as the Federal USAR teams, we all had disparate communications. Further, our communications didn't integrate to the public safety responders, the police, fire, EMTs, dispatch on scene as well, so we had to make extensive use of runners. We had to kind-of come by fly by-wire patching and communications, you know, networks to try to do the best that we could at the time.

Thankfully, like I have mentioned in my testimony, you know, there were some relationships that were already established, so at least we had some kind of idea on who we should reach out to and who we should talk to. Talking with colleagues and counterparts at the Washington, DC aspect of 9/11, it was kind-of the same thing, that they tried to patch everything, and then all of a sudden, everybody was talking to everybody, and nobody could talk.

So probably the biggest success was, again, the bringing all of the efforts together with SAFECOM under what was eventually DHS. SAFECOM had a couple of key models to identify ways to improve governance, equipment, standard operating procedures, training, and exercises. Through those and coordinating the grant funds accordingly, in each of those areas, what we have been able to do since is, through attrition, public safety all across the United States has been able to do a much better job at coordinating as far as our purchases; hey, what are you guys getting, what are we getting, you know, how should we talk, language, you know.

The example that we always use between police and fire, and in your family, I am sure you know how these little debates go between police and fire. Lots of good kidding and ribbing. You know, if the military says cover me, if a firefighter says cover me, and if a police officer says cover me, you can get some very different responses as to what that will mean, whether it is water, whether it is equipment, or whether there are guns being pulled out. So we worked on all of those different aspects.

Again, you know, FirstNet, SAFECOM, the technology is coming, but we didn't get into that position, you know, on September 10. It took a long time to get into the pickle, and it is going to take—continue to take time to get out of it.

Mrs. DEMINGS. Chief, thank you so much for that.

Captain Maier, you talked a little bit in your opening statement about IPAWS and the usefulness of that platform. What would you say are some additional things that can be done to improve the performance of the platform?

Mr. MAIER. One of the most important things that FirstNet has done for us—and can you hear me OK, ma'am? I should check first.

All right. Thank you. My apologies for the earlier technical difficulties.

But with FirstNet, we have to talk about the resiliency of the network and to make sure that the build-out as it is at—I think it is 95 percent complete at this point moving band 14 across the United States, putting that National public safety broadband power in the hands of first responders—that we want to make sure some of that legacy equipment, that the towers are actually built to standards that we would use for our public safety radio systems, that the power systems that back them up, that the diversity of the

paths that actually connect those network of networks together is built to that same standard.

So we see that with FirstNet, they do have a transparency platform with AT&T where I can see, as a first responder, there is help with the network. I can see how things are going. I can see if there is outages or impairments. Here is the thing for us: As first responders, we actually have to anticipate those disruptions and impairments to our operations. We do that all the time, and that includes outages not just related to FirstNet. We plan for those responses, and then during those events, as well as for recovery.

So we know that FirstNet is working with them on this. I have some experience with this. I was part of the FirstNet Public Safety Advisory Committee for many years, served as its vice chair, proud to say that I am very proud of the effort we have seen through the FirstNet Authority and the hard-working people there.

Also think about the deployables that they have put out. They have more than 100 deployables ready to go that can be pre-staged, like they did in the District of Columbia, like they have done in Michigan, to prepare for events, like they have done in Florida and New Orleans. Those are things that we have to be ready for.

I am talking to you from New Orleans right now, and I can see the devastation when I look out the window of what these storms can do and how they can tear up infrastructure. That is what being prepared is doing for us. By partnering with FirstNet and moving this forward, we are building in more resiliency, we are identifying the weak parts, we are ensuring the diversity of the pathways. I am very proud of the work that is going on with it, and it is a very, very useful tool for public safety.

Mrs. DEMINGS. Captain Maier, thank you so much for your response.

The Chair now recognizes the Ranking Member of the subcommittee, the gentlewoman from Florida, for your questions.

Mrs. CAMMACK. Thank you, Chairwoman Demings.

This question is going to be for Sheriff Gator DeLoach, Chief Lombard, and Captain Maier. If you guys could quickly, because I only have 5 minutes, just weigh in yes or no and then elaborate just a little bit.

As you guys know, CISA has cybersecurity advisors deployed across the 10 FEMA regions, and you all have worked with FEMA in one capacity or another, to assist State and local governments and the private sector to help mitigate cyber threats. So my question to you three is, have you had any engagement with the CISA representatives regarding cybersecurity services? If so, has that engagement been beneficial, and how can it be improved?

I will start with you, Sheriff DeLoach.

Mr. DELOACH. Well, my office has not had any personal engagement with CISA. We do have, even for a very rural county, a very robust response to cyber threats that we address through our internal IT staff and also one of the vendors of record that we use here.

Mrs. CAMMACK. Thank you.

Captain Maier.

Mr. MAIER. Thank you, Congresswoman. Yes is the short answer. To expand upon that, I was part of the SAFECOM committee under CISA for many years. I was chair of funding and

sustainment. We took into account building these networks from the bottom up to include cybersecurity so that they are built upon the network of networks security. In fact, one of the things that we have used is that CISA model of really about intrusion detection and intrusion prevention systems and building those in.

The contact with CISA is extensive. I mean, honestly, it would take more than 5 minutes to list it all, but I can tell you they do have the ability to do a technical assistance program that they can actually go out and help identify gaps in what your technology services, especially communications, is doing——

Mrs. CAMMACK. Thank you.

Mr. MAIER [continuing]. As well as some of the COML/COMT stuff.

Mrs. CAMMACK. Excellent. Thank you. Thank you, Captain Maier.

Chief Lombard.

Mr. LOMBARD. Yes. Ranking Member, yes. We actually had the privilege to meet the newly-appointed director, Jen Easterly, and we have had several meetings with Deputy Director Nitin Natarajan, and some great outcomes from that.

You know, being from the home of Amazon and Microsoft, one of the things that we started to do through SAFECOM and working with CISA is start to really foster some of those public-private partnerships, you know, where are some of the expertise and how can we bring some of the talent and the support from the Federal Government together to start addressing public safety needs in this.

Mrs. CAMMACK. Excellent. Thank you, Chief.

Sheriff DeLoach, as you know and we have talked about this several times before, about 60 million Americans or 1 in 5 Americans live in rural America. In fact, 97 percent of America is rural. So, knowing that, and you representing a rural community, can you talk about what it would cost your department to upgrade your radio system?

Mr. LOMBARD. Yes, absolutely. So we have—we are actually in the process of attempting to upgrade our radio system and identify a funding source right now. The long and short of it is, is that it would cost us about $7 million to $8 million to upgrade our radio system and the existing infrastructure. So we are in a position where we can either buy the car or put gas in it, so to speak.

Mrs. CAMMACK. I know we are going to dig into a lot of the nitty-gritty systems themselves in some of the grant funding programs, but something that constantly I believe gets overlooked is the personal human side of what can happen when these radio systems are going down or they don't work.

Have you ever or anyone in your department had a situation where an officer was put in danger or there was a loss of life due to a lack of communications?

Mr. LOMBARD. Fortunately, we have not had a loss of life. However, there are more than we can cover in the short period of time that we have of situations where both fire and EMS crews and deputies were placed in grave harm or peril because of their lack of ability to communicate back with our regional communications center.

Mrs. CAMMACK. Excellent.

I have got about 20 seconds left, so I am going to open it up to all of the witnesses. I think it will probably be hit on later today, but just yes or no in my 10 seconds. You have experienced within your department potentially tragic situations or a tragic situation due to a lack of communication.

Chief Lombard.

Mr. LOMBARD. Yes. There is many examples in the fire service where either radio failures or radio system failures have led to fatalities, lots of reports affirming that.

Mrs. CAMMACK. Captain Maier.

Mr. MAIER. Yes, we had an incident at a shooting scene where departments could not talk to each other. It created a much more dangerous event. It is a terrible situation that could have been averted with better communications.

Mrs. CAMMACK. I appreciate it. Thank you.

With that, I yield back, Madam Chairwoman.

Mrs. DEMINGS. Thank you so much to the Ranking Member.

The Chair will now recognize other Members for questions they may wish to ask the witnesses. In accordance with the guidelines laid out by the Chairman and Ranking Member in their February 3 colloquy, I will recognize Members in order of seniority alternating between Majority and Minority. Members are also reminded to unmute themselves when recognized for questioning.

The Chair recognizes for 5 minutes the gentlewoman from Texas, Ms. Sheila Jackson Lee. Sheila, I know you were on earlier. Is Ms. Jackson Lee still with us?

OK. The Chair will now recognize the gentleman from New Jersey, Mr. Payne, for 5 minutes.

Mr. PAYNE. Thank you, Madam Chair, and thank you for having this hearing, very timely hearing.

I am very pleased to hear the discussion earlier, in the beginning of the hearing, with mention of H.R. 615, the DHS Interoperable Communications Act, which was—I authored that legislation, so I am very proud of that, and also shepherded in the FirstNet operation here at DHS. So it is really good to hear all of that being functioning and active here at Homeland.

Dr. Rodriguez, it is good to see you again. We miss you in Jersey, but it is wonderful that you landed in Washington.

Mr. RODRIGUEZ. Thank you, sir.

Mr. PAYNE. Let's see. So access to emergency alerts and calls are necessary for every American no matter what the economic background or ability. What systems or initiatives does your agency have in place to ensure that all residents receive emergency alerts and information?

Mr. RODRIGUEZ. Congressman Payne, thank you for the question. You are right, and here in the District we do have a diverse socioeconomic resident population, and we did see that certainly in our response to the pandemic but also with some of the disasters and emergencies that we have experienced.

So in addition to some of the tools that I mentioned in my opening statements, we do employ a multifaceted and multimodal approach to disseminating information. I mentioned our Alert D.C.

Campaign, which will go and ping to our resident cell phones either via text or via email.

We also, through the mayor's office and many of our community-based organizations, do a lot of door-to-door canvassing as well directly reaching our residents, particularly in our more disadvantaged wards, wards 7 and 8 in particular.

We also try to reach our residents by getting them to also sign up for some of our telephone notifications. So for residents that don't have cell phones, for example, we can, through our public messaging campaigns, again working with the mayor's office, we are able to reach them in that way so that we can make calls to them during an emergency.

Mr. PAYNE. Thank you. In 2018, a false ballistic missile alert was accidentally issued in Hawaii via the emergency alert system and the wireless emergency alert system. This false alarm caused widespread concern. How can we ensure that such accidents never happen again, and are there current challenges or concerns that you have with the emergency alert system and the wireless emergency alert system?

Mr. RODRIGUEZ. Thank you. I certainly remember that false alarm and alert that was sent out. It did reverberate, I think, across the country and—sorry. For a lot of the witnesses on the line, it was significant.

So what we did here and in my agency actually disseminates the WEA alerts on behalf of the District. So we actually looked at our processes for ensuring that that type of message wouldn't go out. So we do have a layered approach to not only drafting a WEA message but also looking at our geofencing and where we are actually doing it.

I, again, mention the challenges of geofencing. It is not an accurate technology so we do get bleed-over sometimes into Maryland and Virginia, our surrounding counties, which can also be a challenge. But we do have a layered process for ensuring that once the send is hit on the WEA that that has been looked at by several individuals before we actually put out—and vetted before it is put out to the public.

Mr. PAYNE. Well, thank you for those responses.

Madam Chair, I will yield back the balance of my time.

Mrs. DEMINGS. The gentleman yields back. Thank you so much.

The Chair now recognizes the gentleman from Louisiana, Mr. Higgins, for 5 minutes.

Mr. HIGGINS. I thank my friend and colleague, the Chairwoman, and the Ranking Member for holding this hearing today. I thank our law enforcement and first responders for being here today.

Madam Chair, I am concerned about continued endeavors to defund the police. As it relates to today's topic, communications and the effectiveness thereof, here is an example: In Austin, Texas, the police department was defunded to the tune of $150 million. That is about a third of their budget. It is facing quite a crisis. In fact, the Department is now reporting that they are not going to respond to many calls. They have advised the citizens of Austin to dial 3–1–1 for many complaints, including burglaries, suspicious vehicles and people, public disturbances.

Let me clarify that, from Austin's website: When you dial 3–1–1, your call is answered by a friendly and knowledgeable city of Austin ambassador. Our ambassadors are always ready to answer any questions or assist you with any issue you may have regarding the city of Austin's departments or services, 24 hours a day, 7 days a week, 365 days a year. If you dial 3–1–1, you can get an ambassador.

Now, let me just say, when an American citizen is in a bind, they feel like they need to call 9–1–1, they need to be sure—we, the people, need to be certain that there is a police officer on the other end of that phone. The Austin example is quite startling because it is happening across the country in different ways.

After reviewing each of our first responders and law enforcement witness testimonies today, there was a common theme: Every witness here talks about the need for additional resources.

So the answer to improving emergency response efforts, including communications and interoperability across departmental jurisdictional authority, has never been to withdraw resources from our first responders. As a former cop, I can assure the country that defunding the police is the greatest threat to our Nation's ability to respond to emergencies.

Sheriff DeLoach, I am going to ask you a question, and I am going to call you Sheriff Gator DeLoach, because that is the coolest name that has come through this committee in quite some time. According to a post-Katrina FCC report, more than 1,000 cell sites were knocked out, preventing millions of calls from going through. The report goes on to say, a large number of transmission outages also had a huge impact on the ability of public safety systems to communicate.

Your county is susceptible to hurricanes. I have first-hand experience in the challenges that first responders face, that cops face when dealing with the aftermath of a hurricane in communications. Could you please explain to the committee how hurricanes challenge the communications interoperability gap, and how a county sheriff like yourself would respond to those challenges and as that might relate to moves to defund the police. I will yield the balance of my time to you, Sheriff Gator, to answer that question for the country.

Mr. DELOACH. Thank you, Representative Higgins. That is an excellent question. Yes, hurricanes are one of the biggest threats that face our communications infrastructure systems. In fact, that ties directly back in to my testimony, so I will dovetail off of some of that.

Whenever we talk about a regional communications system and regional approaches, we are actually in the process of negotiating with St. Johns County, which is our sister county to the east, to potentially develop a regional communications center which would allow coastal counties like St. Johns to tie into our system or rather us to tie into their system to build additional redundancies and fail safes in the event that we have some type of a catastrophic cell failure, which would allow both entities to continue to operate independent of one another while still depending on the same core or the same common system, if that makes sense.

Mr. HIGGINS. Yes, Sheriff, that makes sense to me.

Madam Chair, I cannot see the clock. I don't know if I have time remaining.

Mrs. DEMINGS. You have 25 seconds left.

Mr. HIGGINS. Thank you, Madam Chair, for the clarification.

Sheriff, could you continue and comment, just talk to America about the challenge that—there is some legitimate argument, you understand, and it is OK for Americans to have this debate. But would you just honestly respond from your perspective to the attempt to defund police across the country?

Mrs. DEMINGS. The gentleman's time has expired, but the witness may answer the question.

Mr. DELOACH. Thank you, Madam Chair.

So, fortunately, living in rural northeast Florida, we don't even have those discussions here. Law enforcement is almost unilaterally respected by our citizens, and we are very grateful for that.

My heart certainly goes out to my brothers and sisters in blue who are experiencing some of those devastating blows to their departments, and certainly even more so to the residents who are suffering at the hands of the funds to—or the attempt to defund police right now. It is un-American, in my opinion, and shouldn't be tolerated.

Mrs. DEMINGS. The Chair now recognizes the gentlewoman from Texas, Ms. Jackson Lee, for 5 minutes.

Ms. JACKSON LEE. I am trying to unmute.

Mrs. DEMINGS. We can hear you now.

Ms. JACKSON LEE. Thank you so very much. Let me quickly——

Mrs. DEMINGS. Ms. Jackson Lee, you are on two different screens. Perhaps if we could eliminate one of them. There is some feedback. I am going to give you a couple of seconds to do that.

Ms. JACKSON LEE. We have eliminated it, I think. We were desperately trying to get on everywhere, but here we are.

Mrs. DEMINGS. That is better. That is better. Go right ahead.

Ms. JACKSON LEE. I still see some jeopardy here so I better talk very fast. First of all, Madam Chair, thank you so very much. [Inaudible]

Mrs. DEMINGS. Ms. Jackson Lee, we continue to have——

Ms. JACKSON LEE. I want to thank you for the committee hearing and the Ranking Member—[inaudible]

Mrs. DEMINGS. Ms. Jackson Lee, we are still having some communication issues. We are going to come back to you. We are going to come back to you.

The Chair will now recognize the gentlewoman from New Jersey, Mrs. Bonnie Watson Coleman, for 5 minutes.

Mrs. WATSON COLEMAN. Thank you. Thank you, Madam Chairwoman, and thank you to the witnesses.

I haven't had a chance to be here for the entire thing because I was double-booked, as life is, but I am very much concerned about this issue. You all represent very different communities, but one thing you all have in common is the vulnerability of being hacked by cyber criminals. Standard communications systems are vulnerable to cyber attacks where encrypted information can be intercepted and copied, and a hacker can attack electronic devices used for information transmission.

So let me ask you, Captain Maier, what are some of your cybersecurity concerns, and do you feel as though DHS has been as supportive as it needs to be with this mission?

Mr. MAIER. Thank you, Congresswoman. That is the best question I have had really related to cyber, what keeps me up at night. Cyber intrusion is a serious threat, and it is a scary consideration that we put this digital data, personal information, all this information that is so essential to criminal justice out on the internet and all these other places and people are hacking in. It is a danger.

So one of the things we have done is we have said, look, these need to be closed systems with controls at entry, controls that have to do with credentialing and management, controls that have to do with understanding the physical layers of the network versus the logical layers of the network, and those are the things that are built into the best systems out there.

We look at some of the work that the CJIS through DHS and through NIST and all of those agencies have really done, and we are talking about risk identification, whether it is assets, data, and those capabilities. Putting that all together for us, we protect it, we detect it, we then respond and then we recover. That is how we do things, and those are the best systems.

But remember, the most important thing is our employees and the people that work for us. We have to do the training, and we have to make sure that they have the information available to say this is a scam, don't respond to that email. We have all seen them—or the telephone calls, and DHS has been on the front of that. Especially having the folks from CISA, they are actually able to work with us in southeast Michigan. It has been very important for us and it is effective.

Mrs. WATSON COLEMAN. Thank you. Thank you, Captain. We want to make sure that you have whatever resources and whatever support that you need from DHS and——

Mr. MAIER. Thank you, ma'am. We appreciate your help and the work of those professionals.

Mrs. WATSON COLEMAN. Well, you know, please know that we are strong supporters of the resources that you need. We are strong supporters of law enforcement across this country, and we don't engage in hyperbole or politicization of the protection of our citizens through its law enforcement.

I have a question for Dr. Rodriguez. Dr. Rodriguez, always good to see you. You know, the attack that took place on January 6 was just sort-of unexpected and—I think it was—I don't know. Maybe—it certainly was unacceptable and it was unexpected with people like me. I personally said, let's go to the Capitol because we will be safe there, and lo and behold, that was like the worst place we could have been on that day.

So Dr. Rodriguez, I want to ask you, could you please describe the current communications operation in our Nation's capital and detail what systems worked on January 6 and what systems caused challenges and where we are in fixing those?

Thank you.

Mr. RODRIGUEZ. Thank you, Congresswoman, and I appreciate the question. It is good to see you as well.

As I mentioned in my opening statements, the FirstNet system did work reliably and consistently on January 6, which I think did assist our first responders, the Metropolitan Police Department, Capitol Police in doing what they needed to do to clear the Capitol of the insurrectionists.

I would also add that there are some, as I mentioned also, our D.C. radio system did work well, as well, on the 6th. We do continue to look for ways that we can better partner with our Federal counterparts, our police, the Capitol Police, in order to make sure that there is that interoperable communications with our Federal partners.

Because oftentimes, you know, with our First Amendment events and special events we host here in the Nation's capital, we do need to make sure that we are able to communicate very quickly with our Federal counterparts because we are called on to support them in many instances.

Mrs. WATSON COLEMAN. Thank you, Dr. Rodriguez.

Madam Chair, how much time do I have?

Mrs. DEMINGS. The gentlewoman's time has expired.

Mrs. WATSON COLEMAN. OK. Can I just close with a question that—can I just close maybe with a comment, because Dr. Rodriguez raised for me something that was really quite significant, in that Washington was ready and able to respond in a timely manner at the point that it knew it needed to respond.

So the question that's still needed to be answered is why weren't we proactively prepared?

Thank you, Madam Chair, and I yield back.

Mrs. DEMINGS. Thank you so much. The gentlewoman yields back.

The Chair now recognizes the gentlewoman from Iowa, Mrs. Miller-Meeks, for 5 minutes.

Mrs. MILLER-MEEKS. Thank you, Madam Chair. Thank you, Ranking Member Cammack.

To all of our witnesses, our first responders, our firefighters, our sheriffs, all of you who are here with us today, it is greatly appreciated the work that you do.

Now, you know, Sheriff Gator DeLoach, you mentioned response to hurricanes and how that affects you. Others of you have mentioned other disasters, how they affect your different regions. In Iowa, we don't get hurricanes unless they are called derechos, which are inland hurricanes.

So some of the comments that I have heard today have talked about resiliency, and I have heard a lot about the FirstNet system and using, you know, cellular communication.

But in a derecho, I can tell you that here in Iowa and central Iowa, in fact, at some of our larger cities, and cellular towers, cellular communication was unavailable. As a State senator, I have, you know, put through legislation for broadband. Our Governor, Governor Reynolds, has just put through $100 million to broadband.

So my question really, and, Dr. Rodriguez, maybe you can answer this or Sheriff DeLoach can answer, you know, in order to have resiliency, should we not have also redundancy of communica-

tions systems, because the same natural or unnatural disaster is not going to affect both areas?

This also leads into the cybersecurity arena as well. You know, what is the possibility of satellites being taken out in outer space? What does that do to our communications system? We have seen U.S. companies purchased by the Chinese Communist Party, and if a Chinese Communist Party purchases a U.S. system or, for example, Huawei and 5G as it is being developed and the challenges with Huawei and security, I think all of these things are important as we develop a communications system and strategy, and hopefully we will see that in this upcoming report.

So if Dr. Rodriguez and Sheriff DeLoach could answer that question briefly, it would be greatly appreciated.

Mr. RODRIGUEZ. Sheriff, I will defer to you and then I will come in after you, if that is all right.

Mr. DELOACH. Certainly, thank you. That is an excellent question. I think one of the key components to focus on here is with the FirstNet build-out, which coincidentally is almost complete in Putnam County, and we are nearing the final stages of completion here.

One of the things that FirstNet brings that makes it so attractive is an additional layer of redundancy above and beyond our land mobile radio system, which allows it to serve as an adjunct to our traditional radio system and even allows us to transmit data that we would normally transmit over our digital land mobile radio systems over cellular or LTE network.

With that in mind and with the particular types of storms that you are talking about, you know, it is difficult to build out some type of infrastructure that could survive some type of a, you know, a catastrophic, really powerful, major hurricane or some type of a 500-year storm. But that was something that FirstNet actually took into consideration whenever they were in the design and engineering phase, so certainly credit goes to them and everyone who had a hand in that.

Mrs. MILLER-MEEKS. Thank you. Before you answer, Dr. Rodriguez, you know, we have recently seen with the outage of Facebook, we know that these types of redundancies are necessary because one communication avenue may be susceptible. So, Dr. Rodriguez, if you would expand upon that and thank you, again, for your testimony.

Mr. RODRIGUEZ. Absolutely. Thank you, Congresswoman. Thank you, Sheriff. We fought—in the District, our interoperability coordinator really develops our plan, and it is really based on the PACE framework, right, the primary which is our radio system, the alternate which is our cell system, our contingencies would be satellite, and then our emergency in a worst-case scenario would be amateur radio runners. So we follow that framework for our communications ecosystem here and certainly with the National Capital Region, and we plan and we train to that.

The other thing I would say is, you know, at the National level—you were talking about State actors too, Congresswoman—I think as the National government, the Federal Government really examines National resiliency, particularly as part of its continuity of the economy framework, as was mandated in last year's NDAA in sec-

tion 9603, I think it is really important for State and local authorities to be part of that planning process and that training process so that they know sort-of at the last mile and how it does impact the residents, States, and local jurisdictions. Thank you.

Mrs. MILLER-MEEKS. These are excellent points. Thank you so much for your testimony.

Madam Chair, thank you for indulging them to answer the questions despite my time having expired, and I yield back.

Mrs. DEMINGS. The gentlewoman yields back.

The Chair now recognizes the gentlewoman from Texas, Ms. Jackson Lee, for 5 minutes.

Ms. JACKSON LEE. Madam Chair, can you all hear me now?

Mrs. DEMINGS. Yes, we can.

Ms. JACKSON LEE. OK. Well, I could have a sense of humor about operating on 2 and 3 and 4 devices trying to get into this hearing, but I was hearing it, and it is an important hearing. So I want to, again, thank you very much for your leadership, two Floridians and the Ranking Member, and I appreciate the fact that we have a combination, very important combination of police departments and fire departments in our Chair and Ranking Member.

I support both in terms of the vital work that they do. Coming from Texas and coming from Houston and being in the eye of disasters, we have had to rely upon the teams working together.

Let me give a brief anecdote as I raise my questions to the witnesses that are there. I was in the United States Capitol on 9/11. I was told by then-Capitol Police, the first voices we heard to get out and run as we saw them doing their job.

It was well-known that the first level of information was not any information, because we did not have the connectedness that we needed. Rumors were that they were headed toward the White House, the Capitol, the State Department, and as well that they were headed to Houston, Texas, because it was the energy capital of the world.

So I first-hand understand clearly, and contrary to my dear friend from Louisiana, Mr. Higgins, that we cities and communities, we support police with funding. We understand and you should understand that there are issues that would involve the George Floyd Justice in Policing Act, but we are supportive of the basic infrastructure of law enforcement in this Nation, and that is all Americans who cede themselves to the authority of law enforcement and first responders, fire departments, as they do their job.

So let me ask this general question that may have been asked but I can ask in a different way. It is all about infrastructure. It is all about the connectedness that you need to communicate. In our visit to 9/11, we were so much reminded of what happened with the firefighters, heroic—running up those stairs and how different systems cannot communicate.

So I understand we are still on the 1960's and 1970's infrastructure. Give us just your point of what we need to do immediately. There is a funding question. There is a technology question. I know that you have been answering, but give it to me in a pointed way so that we can end this in 2021 that you have been in dealing with for this long period of time.

I would be delighted to have the witnesses answer these questions if they would. Do I need to call on the deputy chief of the fire department, Seattle, and then others who could answer? Thank you.

Mr. LOMBARD. Thank you, Congresswoman.

Ms. JACKSON LEE. Chief Lombard, there you are.

Mr. LOMBARD. Thank you, Congresswoman. So one of the things—you mentioned the technology, but I can't emphasize enough the people aspect, that making sure that we have—the people that we know that we have to talk to.

When I went down to Hurricane Harvey, one of the first phone calls I was able to make was to Todd Early, your SWIC, your Statewide interoperability coordinator, and Ken Wright, who works with the Houston Fire Department. By contacting them, I was able to find out who I needed to talk to to find out and facilitate the communications infrastructure, what is working, what is not, what can we bring, how can we help you.

DHS's support of SAFECOM in the FirstNet Public Safety Advisory Committee are two great examples where you, as Congress, are bringing us together so that we can make those connections, make those relationships so that when disaster does come we know who to contact on the ground.

Ms. JACKSON LEE. So Chief Maier, Sheriff Maier, what is your assessment of the greater work that we can do for law enforcement and the connectivity that you need?

Speak about connectivity between different first responders, such as connectivity with fire departments in addition to police departments or law enforcement. Chief Maier.

Mr. MAIER. Thank you, Congresswoman. Go ahead. Oh, I am sorry. Can you hear me OK?

Ms. JACKSON LEE. Yes, I can hear you now.

Mr. MAIER. Sorry. Thank you, ma'am. Congresswoman, thank you for giving me a chance to talk about this. One of the most important things that Deputy Chief Lombard talked about was that communication planning process, and that is a fact. DHS has been a leader on this.

Continued funding and support of SAFECOM, where I served in the funding and sustainment, where we developed how to have radio systems that are not just interconnected but were truly interoperable, because we understood, as you stated, we have to talk to the police, the fire, the EMS, and all of the public safety people that support us, those relationships and in the planning process are the single most important thing to move forward.

Technology can be leveraged, most certainly. We have diversity. We include resilience in our systems. As the sheriff talked about in Florida, we can have alternate locations to have our emergency communications centers, so that if they are affected, they don't take off the entire communications system, just part of it that is affected. We work around those. That is what we plan to do. Your continued support and funding of DHS SAFECOM and the efforts that we are doing will help keep us on the right path forward.

Mrs. DEMINGS. The gentlewoman's time has expired. Thank you so much.

Ms. JACKSON LEE. Thank you so very much for this hearing.

Mrs. DEMINGS. The Chair now recognizes the gentleman from Texas, Mr. Green, for 5 minutes.

Mr. GREEN. Thank you very much, Madam Chair, and I thank the Ranking Member as well. I am very appreciative that we have such outstanding witnesses today to share intelligence with us.

This is one of those times when I think we can all agree that the success of what we are attempting to accomplish is going to be of great benefit not only in terms of interoperability as it relates to fire and police, which is very important, because I was here when Katrina hit. I remember how we had the lack of interoperability at that time, and this is very important.

But also, I am concerned about interoperability as it relates to the general public, because there are times when the lines, the means of communication by way of cell phone, they are oversaturated. That oversaturation leaves the public without an opportunity to ascertain what the salient issues are.

So I am interested in getting some sense of how we are interconnecting with interoperability as it relates to the general public. I will start with Mr. Christopher Rodriguez. Dr. Rodriguez, your thoughts on the public and how we phase the public into all of this, because many times I am being called upon and I can't get through to the people that need to know.

Mr. RODRIGUEZ. Yes, thank you very much, Congressman Green, for the question. I think it is important to look at the public as part of a larger emergency communications ecosystem that of which they are a part of it.

So from our perspective in the District, I mentioned earlier in my comments about the ways that we try to reach the public as a city and actually as a region. We do have a regional watch-and-warn notification team that actually sits in the District that will alert the National Capital Region residents, of which there are nearly 6 million, if you include the District and surrounding counties. So we can reach them.

But also, they need to know how to reach us if there are issues that they need to bring in emergencies or disasters, whether it is reporting suspicious activities or letting us know that, you know, a road is closed or a traffic accident has happened. So we do a lot of communication with the public to make sure they know how to sign up for our alerts, how to get direct feeds from authorities, but also how to communicate with us as well.

Mr. GREEN. Let me share an additional concern. When we have had hurricanes here in Houston, I get a lot of calls to my office about electric wires, power lines that are down, and they are out in the street and they are bouncing around. The public needs to get help—needs to get somebody out to take care of these wires, and they call my office. So there is an additional reason for this. This was the thing that came to mind when it was called to my attention. So that is important.

But let me move on and ask the honorable H.D.—is it DeLoach? DeLoach. Can you comment on this, Sheriff?

Mr. DELOACH. Yes, sir. Just to dovetail on what Dr. Rodriguez was talking about, you know, that presents a significant challenge in a rural community, you know, not unlike your area where we are frequently faced with hurricanes and significant storms. I think

the early warning is key because there is that knowledge we have from past storms that typically there is some infrastructure failures there.

So I think that really what is key to this conversation that early warning and notification prior to the impact of the actual storm so that residents can put protective measures in place and evacuate the areas if they are in low-lying areas.

Not unlike any other place, we use a multifaceted approach when it comes to communication. We rely heavily on social media, an early warning system and also a messaging system and reverse 9–1–1 system to push out those messages. But I think there still needs to be some significant works that is done as far as building redundancy and resiliency into those systems so that they function even when conditions are less than optimal.

Mr. GREEN. Well, I have about 25 seconds left, according to my timer. I don't have the actual timer. So let me just share this thought with you. My uncle was a deputy sheriff, and I attribute my success in life to him because of some sage advice that he gave me.

So I want to let you know how much I appreciate the persons who are in law enforcement, fire departments, the constables, the various members of the constabulary who are out there putting your lives on the line to make sure we are safe. Sometimes you go above and beyond the call of duty even when it is not required for you to go above and beyond the call of it, so thank you very much.

Thank you, Madam Chair, again, for your sage advice that you have given us as we have gone through this process as well. Thank you, everyone.

Mrs. DEMINGS. Thank you so much. The gentleman yields back.

We do have time for a second round of questioning if the Members so desire. I want to thank our witnesses for the outstanding job and information that you have given us today. You know, I will begin with myself.

One of the things that I said in my opening statement was Members of Congress have an important role to play. We have an important role to play, and today we are here to assess our progress over the last 20 years to ensure that our first responders and emergency management personnel have the resources to effectively respond to tragedies and to protect human life, to protect the American people. I thank you for staying focused today on that goal and on that purpose.

We never want a vicious and cowardly attack like we saw on 9/11 to ever happen to us again. That is not a political goal. That should be everybody's goal. So I want to thank you for what you have added to this conversation and the information that you have given us as Members of Congress who are laser-focused on making sure that you have the resources that you need.

A part of that, of course, are the DHS grants. I would just like to ask all of the witnesses, how has the DHS preparedness grants, such as UASI and State Homeland Security Program, helped further develop your communication strategies? I would like to ask all of the witnesses, and, Dr. Rodriguez, we will start with you.

Mr. RODRIGUEZ. Thank you. I appreciate the question, Congresswoman. The preparedness grants are an essential part of our abil-

ity to be interoperable. Since 2003, the National Capital Region has received about $1.2 billion in preparedness grants, of which close to $300 million has been spent to upgrade our radio systems and make them more interoperable.

Most of the—but that doesn't tell the whole story, right, because there are a lot of local budgets that are impacted by having to upgrade radio systems every year, and then we do a large replacement of our regional cash every 10 years. So that cost is about $10 million per year to just do upgrades to the system.

The other challenge that we have, and we appreciate the subcommittee's assistance on this, is, of course, FEMA putting in place mandatory minimums for what we have to spend the grant on. I think as we enter, you know, a period of where we have to be very flexible, the mandatory minimums—which account for about 30 percent of the grants that all the UASI regions get, kind-of put these limits on what it is we can spend on when, in my view, we need to remain flexible and nimble, particularly for State and local jurisdictions.

Mrs. DEMINGS. Thank you so much, Dr. Rodriguez.

Chief Lombard.

Mr. LOMBARD. Thank you very much, Chair. The grants have been phenomenal, and, in fact, they have been absolutely essential, certainly for our region. You know, we are not just buying equipment, although the equipment is very important. We have been able to, you know, get over the hump so to speak as far as speeding up processes to make sure that our radio systems intertwine to all of those radio systems around us at the State, the local, the level, the Tribal level, and whatnot.

But, additionally, they have actually helped us as far as training and exercises. So the equipment is only as good as your ability to know what you are using and working. So we have over the years had multiple training and exercise scenarios where we actually got to use the equipment and practice talking to each other before the big disaster.

Then in the usage, we have been able to use the grants to get together committees to work on policy so that we know, you know, on game day, here is what I need to do, here is where I need to go.

So, again, you know, the policy, the equipment, the usage, putting the governance committees, it has all got to work together. The grants have been instrumental in making that happen, certainly in our region and many like ours.

Mrs. DEMINGS. Thank you.

Sheriff DeLoach, I grew up in a rural part of Jacksonville, in Mandarin. I am sure you are familiar with that area. But I so appreciate what you said the scenario of, you know, the challenges may be different, the amount of support that you get may be different, but you are responding to the same calls, enforcing the same laws. So the level of service that you are expected to give is really the same. Could you talk a little bit about the importance of grants in your area?

Mr. DELOACH. Certainly. Thank you again, Madam Chair. The unfortunate reality is is that typically what we see, at least in Florida, with regard to UASI and DHS monies is that they are typically

funded—or funneled toward the more urban areas down in Broward County and the southern part of the State and even into Duval and Orange Counties.

I understand the importance of protecting those infrastructures and ports and some of the assets that we have in those more populous areas, but sometimes it feels as if some of the more rural areas in Florida and in across the Nation often are overlooked or can't meet the demands of the reporting requirements and other demands the grants place on us.

Mrs. DEMINGS. Thank you, Sheriff.

Last but not least, Captain Maier.

Mr. MAIER. One of the things we see with the UASI funding is it is essential to help us move forward, especially since 9/11. The funding, while it has been reduced, it has stabilized the last few years. We would just ask that you continue funding that moving forward. To align really with what you had said earlier, with 25—[inaudible]

Mrs. DEMINGS. Captain Maier, we are having some audio—are you——

Mr. MAIER. Communications——

Mrs. DEMINGS. OK.

Mr. MAIER. Subcommittee. With the interoperable communications subcommittee, we have seen our amount of that shrink too.

But Chris Lombard is correct; we have addressed more training issues rather than equipment-related. But here is the thing, through that grant guidance we are able to give the best direction possible to avoid those proprietary interfaces and those raw connections for some of these communication packages. We would be in a much better position. Thank you for supporting us on that.

Mrs. DEMINGS. Thank you so much.

The Chair now recognizes the Ranking Member, Mrs. Cammack, for 5 minutes.

Mrs. CAMMACK. Thank you, Madam Chairwoman. You hit on one of the issues that I really wanted to bring to light and discuss today, which is the challenges that some of our rural communities have with these grants. So many of them are really just unattainable from a number of vantage points, one being they don't meet the requirements.

In Putnam County, for example, and Sheriff DeLoach can speak to this, we have the main city Palatka, which is exactly 400 people over the threshold for certain grants for low population areas. So because of that they have the exact same struggles that very small, rural communities have, but that 400 person over the limit has excluded them from a number of grants putting them in a pile to compete with cities like Jacksonville, Orlando, or Miami.

So, Sheriff DeLoach, I would love for you to just touch on this. I just went through about 28 pages of available grants through DHS, and it looks like Putnam County and several of the rural communities—and as was mentioned earlier, you know, 97 percent of America is rural. One in 5 Americans live in rural America. When you look at that list of available DHS grants, communities, and rural communities only are eligible to apply to about 10 to 15 percent of those.

Can you talk about how you guys are getting creative and what we could be doing to open up that grant a little bit more so that we are covering both the urban areas but also the rural communities?

Mr. DELOACH. Certainly. I will say this as a qualifier prior to answering the question, you know, certainly when it comes to grants and reporting requirements, I understand the need for accountability. But whenever I manage an organization like mine where we have 256 full-time employees, a complete complement of 308 full- and part-time employees, it is difficult when you contrast us with someone down in south Florida where they have a staff and several thousand people and perhaps, you know, an entire floor and a building dedicated to management of grants. Unfortunately, those are just resources that we don't have available to us.

Like you just said a few minutes ago, because of the quagmire that we are placed in because of that awkward stage in growth where we are now, it knocks us out of eligibility for many of them. So I would ask each of you to reconsider those eligibility requirements to open them up to some of rural America so that we have access to that money.

Mrs. CAMMACK. Thank you, Sheriff.

This question is for Chief Lombard. So in your testimony you had highlighted that SAFECOM had been critical to improving interoperability. You also highlighted how SAFECOM is one of the first organizations to bring together representatives from public safety associations as well as emergency responders in the field.

Can you talk a little bit more about how important it is to have buy-in from the emergency responders in the field and across all spectrums, rank-and-file, all the way up to management when discussing things like SAFECOM or the National emergency communications plan?

As a caveat to that, can you also talk about, from your perspective, do you think that rural America is represented accurately and adequately in these discussions when you are building this out?

Mr. LOMBARD. Absolutely. So one of the key points that you captured on, Congresswoman, was that, you know, first response is only effective in so much as the secondary response is able to sustain the events. So one of the things that SAFECOM has done that has been so well-received is to actually bring in those other parties.

So, for example, a dear friend of mine, Phillip Mann, who is the public works director at Gainesville, Florida, represents public works throughout the United States, recognizing that, you know, when we are talking about interoperability issues, when we are talking about sustaining the response, the police, fire, and EMS, and 9–1–1 are doing, being able to bring in experts like Director Mann and talk about, OK, if you want to keep the water on the big fire, if you want to keep the roads open—how are we going to be able to, you know, communicate to us and for continuing that dialog?

SAFECOM really strives to maintain a really diverse group as far as, again, Federal, State, local people are brought together, responders are brought together, not just big cities. There is a lot of smaller, more rural areas that are brought together too, because one of the things that we find at the end of the day is that even

though some of us are bigger or smaller, so many of these issues are the same. It is just a matter of scaling.

The western United States, 50 percent or almost 50 percent of the land is all Federal out here, so you don't have to go too far outside of the big cities on the West Coast before you get into some very rural area. As you know, with the wildland fires every year, we are going there a lot.

So it is—again, the—you know, the funding and the support that the Federal Government has gotten or put forth on helping us facilitate those relationships, I think, the bang for the buck that we have been getting is just amazing as far as bringing us together and letting us collectively work our problems out. Hopefully that answers your question.

Mrs. CAMMACK. No, that does.

Thank you, Chairwoman Demings, and thank you to all of our witnesses here today. This is an issue that is important in every single one of our Congressional districts, and we want to make sure that we are working effectively and efficiently in delivering real solutions that meet the needs on the ground. So I look forward to continuing that work. Thank you, Congresswoman Demings and Chairwoman, for allowing a second round of questions.

Mrs. DEMINGS. I want to thank the Ranking Member. Of course, I too look forward to continuing the work with you and other Members of this subcommittee to make sure that we are being responsive to the needs of all America, particularly looking at grant eligibility. So I look forward to that work.

I want to know if there are any additional Members who would like to ask questions? The Chair now recognizes the gentlewoman from Texas, Ms. Jackson Lee, for 5 minutes.

Ms. JACKSON LEE. Thank you, Madam Chair. I would—and thank you again for the hearing, along with the Ranking Member.

I am going to ask Director Rodriguez, and I certainly want to express my appreciation. So obviously, January 6 was an extreme day for all of us, and it drew on everybody for America to see Americans attacking our first responders in a way that it was unspeakable.

But to the coordination question that I am consumed with, I want to ask the question, maybe again, dealing with FirstNet, because you stated ultimately this collaboration and their dedicated bandwidth allowed FirstNet to perform reliably for our first responders on January 6. We are in the process of working with FirstNet to acquire two of our own units, which will contribute and self-sufficiency for the district emergency communications.

I know that you might not pointedly be able to comment, but I do understand amongst our Capitol Police, for example, they were speaking about some interoperability, and it is important that the team in the District of Columbia can all communicate, that would be the Capitol Police, other Federal authorities, and all of you.

Can you just speak to the requiring of more funding so that Congress can—and how we can—I am sorry—approve the funding on how to secure this competency and also with FirstNet, and what you might need. Director? Thank you very much.

Mr. RODRIGUEZ. Yes, thank you, Representative Jackson Lee.

Ms. JACKSON LEE. Dr. Rodriguez.

Mr. RODRIGUEZ. Yes. Can you hear me OK?

Ms. JACKSON LEE. Yes, absolutely.

Mrs. DEMINGS. Representative Jackson Lee, you did have some communication issues, but I hope Dr. Rodriguez was able to hear enough to be able to respond to your question.

Mr. RODRIGUEZ. Yeah, thank you, Representative.

Ms. JACKSON LEE. Did you—OK. Thank you.

Mr. RODRIGUEZ. OK. No problem. So thank you for the question. Certainly, during January 6, as I mentioned, FirstNet did operate consistently and reliably. We—at the time, U.S. Capitol Police was not on FirstNet. Again, any questions about getting them on or what the plan is to do that, I would have to refer to the Capitol Police for that. But I do know that following the 6th of January, we did sort-of reemphasize the importance of communication, of interoperability, but also operational planning.

You will recall, just less than 3 weeks ago, there was a lot of concern over the September 18 protests that were coming to the District, and I know a lot of security was put up around the Capitol. Capitol Police did engage in an extensive interagency effort to make sure that both local, State, and Federal law enforcement agencies were all on the same page.

We did institute and use at that time the National Capital Region's tactical plan, which allowed for interoperability across the radio channels, which really helped us. So we learned a lot from January 6 in terms of communications, so we continue to work with our Federal partners to make sure that we just keep refining and building out that capability.

Ms. JACKSON LEE. So if I might, can you hear me? Would it be helpful that all of the components, including the Capitol Police, have FirstNet in a place that is so visited, so much potential target, and so much a singular entity, which is the Capitol of the United States and certainly the home of the residents of the District of Columbia? How important is that to have that resource?

Mr. RODRIGUEZ. Yes, ma'am, I think it is very important. Any effort that drives us toward greater interoperability and coordination is always a good thing.

Ms. JACKSON LEE. Thank you, Madam Chair.

Mr. RODRIGUEZ. I would also add——

Ms. JACKSON LEE. I will yield back.

Oh, go ahead. Go ahead, Director.

Mr. RODRIGUEZ. I would also just add that, in addition to radio, video and data is also an important component of that as well.

Mrs. DEMINGS. The gentlewoman yields back.

With that, I want to thank all of our witnesses for your invaluable testimony today and for your service every day. I want to thank our Members for their questions.

Additionally, without objection, I would now like to submit a statement for the record from the Major Cities Chiefs Association. The Members of the subcommittee may have additional—the Members—I am sorry. We submit this statement for the record.

[The information follows:]

STATEMENT OF ART ACEVEDO, PRESIDENT, MAJOR CITIES CHIEFS ASSOCIATION

OCTOBER 7, 2021

Chairwoman Demings, Ranking Member Cammack, and distinguished Members of the subcommittee: Thank you for the opportunity to submit this testimony for the record. In addition to being the chief of police in Miami, Florida, I also serve as president of the Major Cities Chiefs Association (MCCA). The MCCA is a professional association of police chiefs and sheriffs representing the largest cities in the United States and Canada.

Last month, we commemorated the 20th anniversary of the 9/11 attacks. We must never forget those who lost their lives on that terrible day. We must continue to honor the brave first responders in New York, at the Pentagon, and in Shanksville who made the ultimate sacrifice to ensure others made it to safety. We must continue to support those heroes, who came from across the country, as they continue to battle health complications and other traumas stemming from their selfless actions during the response and recovery. Finally, we must remain vigilant as the threat environment facing the homeland becomes more complex, so the American people never again experience such tragedy.

Local law enforcement is the front-line response, whether it be a terrorist attack, natural disaster, or global pandemic. Effective communications play a critical role in coordinating and executing the public safety response to a given incident. In the aftermath of 9/11, deficient and non-interoperable public safety communications were identified as shortcomings that needed to be addressed. The 9/11 Commission found that:

"The inability to communicate was a critical element at the World Trade Center, Pentagon, and Somerset County, Pennsylvania, crash sites . . . the occurrence of this problem at three very different sites is strong evidence that compatible and adequate communications among public safety organizations at the local, State, and Federal levels remains an important problem."[1]

While significant progress has been made to improve public safety communications over the last 20 years, there are still several outstanding issues. My testimony will provide a local law enforcement perspective on these remaining challenges and offer a few suggestions on how they may be addressed.

NEXT GENERATION 9–1–1

Nine-one-one systems are critical infrastructure in every community. It is ingrained in us from a young age to dial those numbers if we ever find ourselves in an emergency. Millions of Americans every year depend on these systems to dispatch help in their time of need. Considering the importance of 9–1–1 systems, most people are surprised to learn they are underfunded and technologically inadequate. Many
9–1–1 systems throughout the country rely on decades-old landline technology—things like copper wires and conventional switches. One could reasonably argue that the smartphones we all carry in our pockets are more advanced and have more capabilities than some of the 9–1–1 systems public safety agencies currently operate.

Upgrading our Nation's 9–1–1 systems to Next Generation 9–1–1 (NG 9–1–1) systems is sorely needed and long overdue. NG 9–1–1 will enable faster and more efficient emergency responses, make first responders and the communities they serve safer, and allow law enforcement and public safety professionals to better meet the needs and expectations of the tech-enabled, 21st Century American public. For example, NG 9–1–1 will enable dispatch centers to receive a variety of multimedia and other rich data from callers and seamlessly share it with first responders in the field. The benefits of this capability are endless. Live videos of a crime scene could help law enforcement more quickly identify where a suspect is located. Photos from a burning building can assist firefighters with determining what rescue equipment is needed. Health information sent from a smartphone or smartwatch can assist EMS and hospitals with preparing treatments before a patient is in their care. The ability to utilize advanced data is just one of NG 9–1–1's many benefits. Simply put, upgrading to NG 9–1–1 will save lives.

To help raise awareness and advocate for NG 9–1–1, approximately 2 years ago, the MCCA helped found the Public Safety Next Generation 9–1–1 Coalition. The Coalition consists of the leadership of many of America's major law enforcement, fire

[1] The National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States,* July 24, 2004, pg. 397.

service, emergency medical services, labor unions, and public safety communications associations. The goal of the Coalition is to work with Congress and other key stakeholders to ensure the right policies are in place and secure the requisite resources to bring about a Nation-wide upgrade of existing 9–1–1 systems to next generation systems. As part of its efforts, the Coalition established a set of first principles. These principles must be incorporated into any NG 9–1–1 upgrade to ensure public safety professionals and the communities we serve can realize the full benefits of this technology. The Coalition's first principles are:

- NG 9–1–1 should be technologically and competitively neutral and use commonly-accepted standards that do not lead to proprietary solutions that hamper interoperability, make mutual aid between agencies less effective, limit choices, or increase costs.
- Development of program requirements, grant guidance, application criteria, and rules regarding NG 9–1–1 grants should be guided by an advisory board of public safety practitioners and 9–1–1 professionals.
- NG 9–1–1 must be fully funded to ensure it is deployed throughout the country in an effective, innovative, and secure manner and to enable NG 9–1–1 implementation training Nation-wide.
- The process for allocating funds to localities should be efficient, Federal overhead costs should be minimized, and grant conditions should not be onerous or extraneous and should be targeted to achieve important objectives including interoperability and sustainability.
- Cybersecurity of NG 9–1–1 systems should be a primary consideration.
- Incentives for increased efficiency of NG 9–1–1 functions, including through shared technology and regional collaboration, should be included.

While all the Coalition's first principles are important, I want to focus on interoperability. A lack of interoperability is one of the most significant flaws with current 9–1–1 systems, as 9–1–1 centers cannot quickly transfer calls to other centers. Instead, public safety communications professionals typically need to facilitate the transfer manually. As a result, the individual who called for help often needs to tell their story again to the dispatcher at the new center. Every second counts when responding to an emergency, and the delays created by a lack of interoperability can be the difference between life and death.

Roughly 80 percent of 9–1–1 calls are now made from cell phones. In many instances, the 9–1–1 center that receives the call is based on the location of the cell tower that processed the call. It should be noted that while wireless carriers and device manufacturers have developed and implemented features to route calls based on the device's actual location, it is not always possible to direct calls via this method.[2] MCCA member agencies typically border multiple jurisdictions, which complicates the challenges related to interoperability. MCCA members can provide numerous examples of calls for service in their cities, especially near jurisdictional boundaries, being routed to 9–1–1 centers in neighboring areas. One member located near the State line has indicated that emergency calls are sometimes routed to a 9–1–1 center in another State.

The upgrade from landline to IP-based technology, known as ESInets, is the backbone of an NG 9–1–1 upgrade. This is an important step but is not enough on its own to solve interoperability issues. As 9–1–1 systems are upgraded to NG 9–1–1, these new systems must be technologically and competitively neutral. NG 9–1–1 systems also must use commonly accepted standards and cannot rely on proprietary solutions. If we fail to do this, we risk ending up in a situation that shares many of the challenges public safety agencies are currently experiencing with land mobile radios. I will discuss those issues in greater detail later in my testimony.

Traditionally, 9–1–1 operations are a State and local function. Unfortunately, this has created a situation of "haves and have-nots," where 9–1–1 system capabilities vary dramatically between States and communities. Given the immense public safety value, we must ensure that all of America, from the largest cities to the most rural counties, can upgrade to NG 9–1–1 systems as soon as possible. It will be tough to efficiently implement this upgrade Nation-wide without an investment of Federal resources. The cost of this upgrade goes well beyond the infrastructure and technology NG 9–1–1 systems need to operate. There are also costs associated with other critical components, such as training dispatchers and other personnel on these new systems and implementing vital cybersecurity measures to ensure the systems cannot be taken off-line by malicious actors. Federal assistance for NG 9–1–1 systems must be sufficient enough to address all aspects of the upgrade. Otherwise,

[2] Mark Reddish, "New Progress for Getting Wireless 9–1–1 Calls to the Right ECC," APCO International, September 26, 2019. *https://www.apcointl.org/2019/09/26/new-progress-for-getting-wireless-9-1-1-calls-to-the-right-ecc/*.

it may further cement the status quo of "haves and have-nots." It may also inhibit public safety from addressing all existing challenges with current 9–1–1 systems or fully capitalizing on the new capabilities NG 9–1–1 systems provide.

The Coalition worked closely with the House, Senate, and other stakeholders to secure funding for NG 9–1–1 in the reconciliation package that Congress is developing. These resources will be instrumental in ensuring that all communities have a secure, resilient, interoperable, and reliable way of receiving, processing, and responding to requests for emergency assistance. The MCCA strongly encourages all Members of Congress to support the NG 9–1–1 portion of this legislation.

RADIO INTEROPERABILITY

Land mobile two-way radios are law enforcement officers' primary communication tool. During calls for service, officers rely on their radios to stay connected and share and receive information with dispatch centers, command staff, and other officers in the field. The ability to communicate seamlessly helps ensure that the law enforcement response to an emergency is as effective and safe as possible for all parties involved.

While there are few issues with intra-agency communications, interagency communications can be complex, especially among agencies using conventional radio systems. Conventional radios use radio bands that are typically based on the user's operational needs. For example, police departments in metropolitan areas may use ultra-high frequency (UHF) radios due to UHF's ability to permeate buildings. However, departments in rural areas might use very high frequency (VHF) radios due to VHF's ability to transmit information over long distances. Conventional systems are not interoperable, as an agency using a UHF system cannot communicate with an agency utilizing a VHF system without deploying additional technology, often at great expense.

Considering these challenges, many MCCA member agencies have developed and implemented workarounds to facilitate interagency communications. These solutions do have some shortcomings that can impact their effectiveness. One workaround is to install patches that allow radio systems to take incoming communications from one band and rebroadcast them out on another band. However, for an officer to receive these communications, they must be in range of a radio tower or repeater that uses the same band as their radio. This may result in a loss of interoperability if the officer is outside of their usual area of operations.

The workarounds to achieve interoperability are also incredibly expensive, which limits how widely agencies can deploy them. For example, one MCCA member purchased dual-band radios that could utilize UHF and VHF but could only afford to put them in patrol cars. Therefore, these officers lose access to interoperable communications as soon as they leave their vehicles. While these kinds of solutions do represent some progress, they do not represent full interoperability. Despite the 9/11 Commission's recommendation, challenges related to interoperability have simply been patched, not solved.

The lack of interoperable communications can present several operational challenges whenever multiple agencies are responding to an incident. This is especially troubling for the MCCA, as our member agencies operate in major urban centers with numerous other law enforcement and public safety agencies. MCCA members work closely with these agencies to facilitate mutual aid requests and respond to incidents that cross-jurisdictional boundaries. Furthermore, police often respond jointly with our fire department and EMS colleagues to traffic accidents, fires, and medical emergencies. The inability to easily communicate with each other adds yet another layer of complexity to these joint responses.

Public safety agencies would significantly benefit by moving from conventional to digital radio systems. Digital systems create efficiencies and allow more users to operate on fewer frequencies. Most importantly, the transition from conventional to digital systems provides a pathway to full interoperability. Despite this pathway, there are still several hurdles that need to be overcome. The current industry standard, P25, has produced a situation that lends itself to proprietary vendor solutions. Consequently, digital radio systems are often only interoperable if both parties use the same vendor. To communicate with systems developed by other vendors, agencies need to purchase special, expensive, technology called gateways.

There undoubtedly is a need for public safety, industry, the Federal Government, and other stakeholders to work together to address the shortcomings in the current standards. The MCCA stands ready to help advance these conversations. Any updated standards must eliminate proprietary solutions, which inhibit interoperability. They must also address emerging issues such as encryption. Currently, radio systems that use different encryption standards are not interoperable, even with a

gateway. If systems used commonly accepted encryption standards, it would help eliminate this challenge.

Upgrading to digital radio systems requires significant resources, as it often necessitates a complete rebuild of the radio system. The costs include not only the radios themselves but also the purchase and installation of additional radio towers, repeaters, and other infrastructure. One MCCA member, located in a smaller jurisdiction, estimated that transitioning to a digital radio system would cost the agency $30 million. Most public safety agencies, especially law enforcement agencies, do not have this kind of funding available in today's budgetary environment. It will be nearly impossible to achieve full communications interoperability without assistance from the Federal Government. Congress should consider appropriating additional grant funding to assist State and local entities with upgrading their radios to digital systems.

COMMUNICATIONS RESILIENCY

Emergencies communications, such as 9–1–1 calls, is one of the primary methods through which members of the public let police, firefighters, EMS, and other first responders know they need help. As such, the systems used to receive and manage these communications must be resilient and able to withstand all manner of threats, whether they be natural or man-made.

Unfortunately, just a few weeks ago, the impacts of Hurricane Ida made it abundantly clear that there is still work to do to harden and make our communications systems as resilient as possible. It was widely reported that the 9–1–1 center in New Orleans was off-line for approximately 13 hours following the hurricane.[3] This outage was particularly devastating, considering the sheer number of people who needed assistance during this time. We commend our MCCA colleague, Superintendent Shaun Ferguson, and all the brave officers in the New Orleans Police Department for their efforts to continue to serve their community and aid those in need in the face of this extraordinary challenge.

The outage in New Orleans was attributed to outdated technology. As mentioned earlier, many communities across the United States still rely on landline technology to deliver 9–1–1 calls, which can be especially susceptible to some of the consequences of natural disasters, such as flooding and power outages. The move to NG 9–1–1, where requests for assistance are delivered via IP-based technology, would help alleviate this issue because it would be easier to route incoming calls to another 9–1–1 center. The events in New Orleans are just another example of why it is so important to upgrade our country's 9–1–1 systems to next generation systems as quickly as possible.

Natural disasters are not the only threat that can test the resiliency of public safety communications systems. These systems must also contend with man-made threats, such as cyber attacks. Over the past decade, public safety agencies, including many MCCA members, have experienced increased ransomware, denial of service, and other types of cyber attacks. According to a compilation of publicly reported incidents, there have been 105 cyber attacks directed at public safety agencies in the last 24 months. Several of these attacks were directed at 9–1–1 services.[4] It is important to note this only includes publicly-reported incidents, the actual number of attacks is likely much higher.

As law enforcement and other public safety agencies rely more and more on technology systems to carry out their missions, these attacks can have catastrophic effects. Agencies can be especially vulnerable if their technology systems are outdated, or their personnel are not adequately trained to mitigate cyber threats. These challenges can be exacerbated by public safety agencies' connections with more extensive municipal networks, which may be less secure and provide an alternative vector for attacks.

Public safety must continue to work tirelessly to mitigate cyber threats. One of the best defenses is to ensure that agency personnel are well educated and trained on good "cyber hygiene." Congress can also take a few steps to help local governments defend themselves against cyber attacks. First, Congress must ensure the grant programs that help build local cyber capacity, such as the Homeland Security Grant Program, are fully funded. Congress should also continue to ensure agencies such as DHS's Cybersecurity and Infrastructure Security Agency (CISA) have the

---

[3] Todd C. Frankel, Aaron Gregg, and Drew Harwell, "911 calls after Ida went unanswered in New Orleans due to 'antiquated technology,'" *The Washington Post,* August 30, 2021. *https://www.washingtonpost.com/business/2021/08/30/orleans-ida-911-calls/*.

[4] Seculore Solutions, "Cyber Attack Archive," accessed on October 5, 2021. *https://www.seculore.com/resources/cyber-attack-archive*.

authorities and resources needed to continue programs and efforts designed to help local government agencies prevent and respond to cyber attacks.

LOCATION ACCURACY

When an individual places a 9–1–1 call, dispatchers can typically determine the caller's horizontal location (x- and y-axis) using GPS coordinates that provide the longitude and latitude. While this directs law enforcement and other first responders to a place on the ground, it can be difficult for the dispatcher to determine the caller's vertical location (z-axis). The lack of accurate vertical location data presents an operational challenge, especially for MCCA member agencies, which operate in dense metropolitan areas and frequently respond to calls for service at multistory buildings. In a profession where seconds matter, the amount of time it takes to determine if the person who needs help is on the 5th floor or the 50th floor can have tragic consequences.

Progress is being made, albeit slowly, to improve location accuracy. In 2015, the Federal Communications Commission (FCC) adopted new rules that require wireless carriers to provide either vertical or dispatchable location information (floor level, room number, etc.) to help identify a 9–1–1 caller's specific location. To comply with the FCC's latest order on this topic, the Sixth Report and Order, carriers would have needed to provide this information for 9–1–1 calls originating in each of the top 25 U.S. markets by April 2021. However, they missed this deadline, and the FCC launched enforcement investigations shortly thereafter.[5]

The FCC reached a settlement with the wireless carriers, and the carriers were given another year to comply with the FCC's rules. In addition, the carriers were required to immediately begin providing any available vertical location data.[6] Unfortunately, in many instances, 9–1–1 centers are either unable to receive this data, or the information is too inaccurate to use. Given the public safety benefits, we must continue to improve location accuracy as quickly as possible. As such, through its oversight efforts, Congress must ensure the FCC continues to work with all stakeholders to uphold the commitments and time lines laid out in the FCC's rules.

COMMUNICATIONS GRANT FUNDING

Public safety communication systems are very costly to develop, acquire, maintain, and upgrade. Given the current strain on local budgets, Federal grants can provide critical resources for agencies looking to enhance their communications capabilities. There are numerous grant programs, including FEMA's Urban Area Security Initiative (UASI) and State Homeland Security Grant Program (SHSP), that can be used to fund communications projects. Nevertheless, it is the primary focus of few, if any, of these programs. As a result, communications projects may need to compete with other priorities and projects for grant dollars. UASI and SHSP are two relevant examples that demonstrate how even though a grant program can be used for emergency communications projects, several factors may impact how much of the funding is used for that purpose.

Each year, UASI and SHSP grantees are required to dedicate a certain percentage of funds to projects that meet the criteria outlined in the statute or the grant program's Notice of Funding Opportunity. The percentage of a recipient's award that must be dedicated to these obligations has continued to grow annually. For example, in fiscal year 2020, grantees were required to commit 20 percent of their funding to National Priorities Areas, and in fiscal year 2021, this requirement rose to 30 percent. Since emergency communications do not fall into any of the National Priority Areas, reducing the discretionary funding available for projects outside of these priorities may inhibit agencies' ability to fund communications projects using UASI or SHSP grants. While National Priorities Areas can help ensure limited grant funding is used as effectively, they must be developed in consultation with key stakeholders to ensure the priorities reflect the needs of grantees.

Further complicating matters is that the UASI and SHSP set aside that can be used for communications projects, the Law Enforcement Terrorism Prevention Activities (LETPA), has been weakened over the years. LETPA was initially a standalone grant program but stopped receiving funding in 2007. Now, it is a 25 percent carve-out for UASI and SHSP funds. The move from grant program to spending re-

[5] "FCC Secures Life-Saving Commitments from Wireless Carriers to Deliver 911 Vertical Location Information Nationwide Within Seven Days", Federal Communications Commission, June 3, 2021. *https://docs.fcc.gov/public/attachments/DOC–372980A1.pdf*. See also Page 5 of the FCC Settlements with the wireless carriers, available here: *https://www.fcc.gov/document/fcc-secures-911-vertical-location-commitments-wireless-carriers*.

[6] Ibid.

quirement reduced the available LETPA funding, thereby impacting the universe of LETPA-funded projects. For example, funding for a fusion center and Chemical, Biological, Radiation, Nuclear, and Explosive response teams take up nearly all of one MCCA member's LETPA set-aside every year. Strengthening LETPA, or restoring it to a stand-alone program, may increase the amount of funding available to public safety agencies for emergency communications projects.

CONCLUSION

Public safety communications are an integral part of law enforcement and other first responders' everyday operations and response to emergencies. While some progress has been made since the 9/11 Commission issued its recommendation regarding public safety communications nearly 20 years ago, there are still challenges that must be overcome, especially with respect to interoperability and our country's 9–1–1 systems. Federal assistance will almost certainly be needed if we are to address these issues quickly and efficiently. The MCCA stands ready to work with the committee to address our members' public safety communications challenges.

Mrs. DEMINGS. The Members of the subcommittee may have additional questions for the witnesses, and we ask that you respond expeditiously in writing to these questions. Under committee rules, the subcommittee record shall be kept open for 10 days.

Without objection, the subcommittee stands adjourned. Thank you, all.

[Whereupon, at 1:57 p.m., the subcommittee was adjourned.]

# 20 YEARS AFTER 9/11: EXAMINING EMERGENCY COMMUNICATIONS, PART II

**Tuesday, November 2, 2021**

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON EMERGENCY PREPAREDNESS,
RESPONSE, AND RECOVERY,
*Washington, DC.*

The subcommittee met, pursuant to notice, at 10:02 a.m., via Webex, Hon. Val Demings [Chairwoman of the subcommittee] presiding.

Present: Representatives Demings, Jackson Lee, Payne, Green, Watson Coleman, Cammack, Higgins, Miller-Meeks, and Garbarino.

Mrs. DEMINGS. The Subcommittee on Emergency Preparedness, Response, and Recovery will come to order. The subcommittee is meeting today to receive testimony on "20 Years After 9/11: Examining Emergency Communications Part II." Without objection, the Chair is authorized to declare the subcommittee in recess at any point.

Good morning. Two months ago, we observed the 20-year mark since 9/11, the worst terrorist attack experienced on U.S. soil. In remembrance of that tragic day and the lives lost, the Committee on Homeland Security has been examining what happened that day and how our National security fares today.

In October, this subcommittee held a hearing to examine the progress made in emergency communications since 9/11, focusing on challenges that emergency managers and first responders faced 20 years ago and have continued to face in the 2 decades following. During that hearing, we received testimony from a city emergency manager, a police chief, a country sheriff from a rural area, and we also heard from a fire chief who served at Ground Zero for 2 weeks following 9/11.

Each witness provided valuable insight into the issues we have faced over the years with emergency communications, including interoperability, power outages, outdated 9–1–1 systems, and issues with emergency alert systems. As a former chief of police and first responder, I was honored to have first responders share their expertise and their on-the-ground experiences with this subcommittee.

Today, this subcommittee is taking the conversation we have started with the emergency managers and first responders and continuing the examination of emergency communications challenges with our Federal partners. We have seen vast improvements in the

Nation's emergency communications apparatus through the establishment of programs such as the Integrated Public Alert and Warning System, IPAWS, the First Responder Network Authority, FirstNet, and the Emergency Communications Division.

However, as technology continues to evolve, we must ensure that these programs and their platforms are able to evolve with it. Established in 2006, IPAWS allow Federal, State, territorial, Tribal, and local governments to provide a wide range of alerts to the public in the event of an emergency. There have been multiple updates to IPAWS, including the 2012 modernization steps including enabling authorized Federal, State, territorial, Tribal, and local authorities to send wireless emergency alerts to mobile devices. Additionally, in 2019, IPAWS continued to make improvements by including several enhancements to the system, including increased maximum character count in messages, added support for Spanish language alerts, and improved geographic accuracy.

However, with these enhancements, there has still been challenges that need to be addressed. Inappropriate use of the system has shown to be an issue with the IPAWS system contributing to panic and confusion. We all remember January 2018 Hawaii faced a false alert that stated a missile was headed toward the State causing chaos. Though resolved as a false alarm, it took nearly 40 minutes for officials to release a retraction statement.

In addition to public alerts, a major component to emergency communications is the network used for emergency correspondence among different agencies. FirstNet authority allows first responders to communicate with one another on a dedicated platform. With 95 percent of its network having been deployed Nation-wide, FirstNet has been widely praised by first responders for its reliability in emergency situations.

However, threats to the homeland by the way of natural and man-made disasters can still cause outages. On Christmas day of 2020, a bomb was detonated in downtown Nashville, Tennessee, disrupting phone, internet, 9–1–1 call centers, and FirstNet. It is imperative that we continue to harden our technology and ensure our communications networks are resilient from all hazards.

Though communications, public alerting, and resilient infrastructure are priorities for this subcommittee, the public may only experience their benefit or challenges during times of crisis. Today's hearing will serve as an important forum to continue the conversation on the current state of emergency communications systems and any gaps that may persist.

I am grateful for the participation of our witnesses here today and I look forward to your testimony.

[The statement of Chairwoman Demings follows:]

STATEMENT OF CHAIRWOMAN VAL DEMINGS

NOVEMBER 2, 2021

Two months ago, we observed the passing of 20 years since 9/11, the worst terrorist attack experienced on U.S. soil. In remembrance of that tragic day and the lives lost, the Committee on Homeland Security has been examining what happened that day and how our National security fares today.

In October, this subcommittee held a hearing to examine the progress made in emergency communications since 9/11, focusing on challenges that emergency managers and first responders faced 20 years ago and have continued to face in the 2

decades following. During that hearing, we received testimony from a city emergency manager, a police chief, a county sheriff. We also heard from a fire chief who served at Ground Zero for 2 weeks following 9/11. Each witness provided valuable insight into the issues we have faced over the years with emergency communications, including interoperability, power outages, outdated 9–1–1 systems, and issues with emergency alerting. As a former chief of police and first responder, I was honored to have first responders testify before the subcommittee.

Today, this subcommittee is taking the conversation we started with the emergency managers and first responders and continuing the examination of emergency communications challenges with our Federal partners. We have seen vast improvements in the Nation's emergency communications apparatus through the establishment of programs such as the Integrated Public Alert & Warning System (IPAWS), the First Responder Network Authority (FirstNet Authority), and the Emergency Communications Division. However, as technology continues to evolve, we must ensure that these programs and their platforms are able to evolve with it.

Established in 2006, IPAWS allows Federal, State, territorial, Tribal, and local governments to provide a wide range of alerts to the public in the event of an emergency. There have been multiple updates to IPAWS, including the 2012 modernization steps of including enabling authorized Federal, State, territorial, Tribal, and local, authorities to send Wireless Emergency Alerts (WEAs) to mobile devices. Additionally, in 2019, IPAWS continued to make improvements by including several enhancements to the system including increased character maximum character count in messages, added support for Spanish-language alerts, and improved geographic accuracy.

However, with these enhancements, there are still challenges that need to be addressed when using IPAWS. Inappropriate use of the system has shown to be an issue with the IPAWS system, contributing to panic and confusion. In January 2018, Hawaii faced a false alert that stated a ballasting missile was headed toward the State, causing chaos. Though resolved as a false alarm, it took nearly 40 minutes for officials to release a retraction statement.

In addition to public alerts, a major component to emergency communications is the network used for emergency correspondence among different agencies. FirstNet Authority allows first responders to communicate with one another on a dedicated platform. With 95 percent of its network having been deployed Nation-wide, FirstNet has been widely praised by first responders for its reliability in emergency situations. However, threats to the homeland by way of natural or man-made disasters can still cause outages. On Christmas day 2020, a bomb was detonated in downtown Nashville, Tennessee disrupting phone, internet, 9–1–1 call centers, and FirstNet.

It is imperative that we continue to harden our technology and ensure our communication networks are resilient from all hazards. Though communications, public alerting, and resilient infrastructure are priorities for this subcommittee, the public may only experience their benefit—or challenges—during times of crisis. Today's hearing will serve as an important forum to continue the conversation on the current state of emergency communications systems and any gaps that may persist.

Mrs. DEMINGS. The Chair now recognizes the Ranking Member of the subcommittee, the gentlewoman from Florida, Mrs. Cammack, for an opening statement.

Mrs. CAMMACK. Well, thank you so much, Chairwoman Demings for convening this hearing today to continue our very important discussion about emergency communications. Last month, this subcommittee had the privilege of hearing from several local first responders about the communication challenges that they face every single day. Now, before I begin discussing some of the challenges, I would like to take a moment to highlight the very real human element when talking about emergency communications.

Lack of communication can put our first responders' lives in danger. As we heard, a radio system failure has led to first responders losing their lives. I have said this before, but as the wife of a first responder, this very real scenario is truly unimaginable to me. I want to thank all of our witnesses here today for your dedication to helping improve these vital communication systems as your work really does help save lives.

Now, during our previous hearing, one of the points that really stuck with me is how the needs of rural communities across the country are often overlooked. About 60 million, or 1 in 5 Americans live in rural areas. While these rural communities face many of the same challenges as larger more urban communities, rural communities are also faced with additional challenges brought on by a lack of available resources and funding. One of the local sheriffs from my district, Putnam County Sheriff Gator DeLoach testified at the hearing that his department is still using an antiquated radio system based on technology developed during World War II. This antiquated system effectively isolates them with no ability to communicate with their counterparts as they frequently work with or rely on for assistance. This also puts our constituents in grave danger.

Sheriff DeLoach went on to testify that it would cost his department about $7- or $8 million to update their current radio system. The cost of updating their current radio system is made even more difficult when we consider that more often than not, available grant funding is tailored toward larger, more urban communities. For example, Palatka, the seat, the county seat, for which Sheriff DeLoach serves, is exactly 400 people over the threshold to be considered a low population area for many of the available grant programs. This means that Palatka must compete with larger cities like Jacksonville, Orlando, or Miami.

In addition to discussing the challenges facing first responders in rural communities, we also heard testimony about the importance of strengthening our cybersecurity infrastructure. While I mentioned this last hearing, it is a statistic that I feel needs repeating. A recent survey conducted by SAFECOM found that over one-third, one-third of organizations indicated that cybersecurity incidents have had an impact on their ability of their emergency response providers' and Government officials' ability to communicate over the past 5 years. Now, when we are talking about cybersecurity, it is important to also discuss the important role that NextGen 9–1–1 will play in the future. Providing faster and more reliable response efforts is paramount.

In closing, I would like to recognize the significant progress that has been made to first responder communications since the initial recommendations by the 9/11 Commission. SAFECOM, which is managed by CISA, has been critical to improving interoperability and is one of the first organizations to bring together representatives from public safety associations, as well as emergency responders in the field. FirstNet, established in 2012 by the Middle Class Tax Relief and Job Creation Act, has set some very aggressive benchmarks for the rural deployment of a new first responder communication infrastructure. I look forward to discussing more of that today.

Last, IPAWS provides life-saving information to individuals about severe weather, power outages, and law enforcement situations. In 2012, twice the number of State, local, territorial, and Tribal agencies used IPAWS to reach their constituents when compared to 2019. This further ensures the safety of all Americans.

Finally, in my role as Ranking Member of this subcommittee, I remain committed to ensuring that our policies take into account

the unique needs of our first responders, especially those in rural communities. I look forward to hearing from our witnesses today and working together to improve first responder communications. Thank you again, Chairwoman Demings. With that, I yield back.

[The statement of Ranking Member Cammack follows:]

STATEMENT OF RANKING MEMBER KAT CAMMACK

I would like to thank Chairwoman Demings for convening this hearing today to continue our very important discussion about emergency communications.

Last month, this subcommittee had the privilege of hearing from several local first responders about the communication challenges they face every day. Before I begin discussing some of these challenges, I would like to take a moment to highlight the very real human element when talking about emergency communications.

Lack of communication can put first responders' lives in danger, and as we heard, a radio system failure has led to first responders losing their lives. I've said this before, but as the wife of a first responder, this very real scenario is truly unimaginable to me. I want to thank all the witnesses here today for your dedication to helping improve these vital communication systems, as your work really does help save lives.

During our previous hearing, one of the points that really stuck with me is how the needs of rural communities across the country are often overlooked.

About 60 million or 1 in 5 Americans live in rural areas. While these rural communities face many of the same challenges as larger, more urban communities, rural communities are also faced with additional challenges brought on by lack of available resources and funding.

One of the local sheriffs in my district, Sheriff DeLoach, testified at the hearing that his department is still using an antiquated radio system based on technology developed during World War II. This antiquated system effectively isolates them, with no ability to communicate with their counterparts that they frequently work with or rely on for assistance.

Sheriff DeLoach went on to testify that it would cost his department around $7- to $8 million to update their current radio system.

The cost of updating their current radio system is made even more difficult when we consider that more often than not, available grant funding is tailored toward larger communities.

For example, Palatka, which is the county seat for where Sheriff DeLoach serves, is exactly 400 people over the threshold to be considered a low-population area for many of the available grant programs. This means that Palatka must compete with larger cities like Jacksonville, Orlando, or Miami for funding.

In addition to discussing the challenges facing first responders in rural communities, we also heard testimony about the importance of strengthening our cybersecurity infrastructure. While I mentioned this last hearing, it's a statistic that I feel needs repeating.

A recent survey conducted by SAFECOM found that, "over a third of organizations indicated that cybersecurity incidents have had an impact on the ability of their emergency response providers and government officials' ability to communicate over the past 5 years."

When talking about cybersecurity it is also important to discuss the important role that NextGen 9–1–1 will play in the future. Providing faster and more reliable response efforts is paramount.

In closing, I would like to recognize the significant progress that has been made to first responder communications since the initial recommendations made by the 9/11 Commission.

SAFECOM, which is managed by CISA, has been critical to improving interoperability and is one of the first organizations to bring together representatives from public safety associations as well as emergency responders in the field.

FirstNet, established in 2012 by the Middle Class Tax Relief and Job Creation Act, has set some very aggressive benchmarks for the rural deployment of new first responder communication infrastructure, and I look forward to discussing that more today.

Last, IPAWS provides life-saving information to individuals about severe weather, power outages, and law enforcement situations. In 2020, twice the number of State, local, territorial, and Tribal agencies used IPAWS to reach their constituents when compared to 2019. This further ensures the safety of all Americans.

In my role as Ranking Member of this subcommittee, I remain committed to ensuring that our policies take into account the unique needs of our first responders,

especially those in rural communities. I look forward to hearing from our witnesses today and to working together to improve first responder communications.

Mrs. DEMINGS. I thank the Ranking Member for her statement. Members are also reminded that the committee will operate according to the guidelines laid by the Chairman and Ranking Member in their February 3 colloquy regarding remote procedures. Without objection, Members not on the subcommittee shall be permitted to sit and question the witnesses. Additional Member statements may be submitted for the record.

[The statement of Chairman Thompson follows:]

STATEMENT OF CHAIRMAN BENNIE G. THOMPSON

NOVEMBER 2, 2021

The September 11, 2001, terrorist attack revealed critical problems with our emergency communications systems. Over 20 years later, we have made great strides in our technology and capabilities, but more remains to be done. On October 7, first responders testified before the subcommittee and spoke highly of these advancements and how they have helped strengthen our emergency communications systems. Two of these advancements include the creation of the First Responder Network Authority (FirstNet Authority) and the Integrated Public Alert and Warning System (IPAWS).

Director Chris Rodriguez of the District of Columbia Homeland Security and Emergency Management Agency testified that collaboration and dedicated bandwidth "allowed FirstNet to perform reliably for our first responders at the U.S. Capitol on January 6th." While FirstNet has proved to reliable for the District, there are on-going issues, such as interoperability, outages, and off-network challenges. For example, we have seen interference with wireless communications during large-scale natural disasters, such as wildfires or hurricanes.

When Hurricane Ida hit Louisiana, AT&T's cell towers were down for nearly 2 days after the storm, which crippled communications, including FirstNet. As a result, first responders struggled to communicate with one another, which undoubtedly hurt their response efforts. The ability to communicate during a disaster is of the utmost importance, and we need to address these gaps and mitigate their impact on emergency communications.

IPAWS, which FEMA administers, is designed to improve public safety through the rapid distribution of emergency messages to as many people as possible over as many communications devices as possible in the event of a disaster. FEMA designed IPAWS to integrate future technologies into the platform so it could improve as technology advances. I hope to hear today how IPAWS has matured and improved communication for communities during emergencies.

Additionally, the Emergency Communications Division at the Cybersecurity and Infrastructure Security Agency (CISA) has made strides in our emergency communications apparatus through the Safer America Through Effective Public Safety Communications (SAFECOM), which provides guidance and assistance to those using the Homeland Security Grant Program funding to buy emergency communications items. While technology has improved in the last 20 years, we must ensure that as the threat landscape evolves, there continues to be adequate focus and funding for communications infrastructure.

I look forward to hearing from our witnesses today about how their organizations are confronting communications challenges and learning what the Committee on Homeland Security can do to aid them in making our Nation safer.

I now welcome our panel of distinguished witnesses. Our first witness is Mr. Antwane Johnson, the director of the Integrated Public Alert and Warning Systems of the Federal Emergency Management Agency. Mr. Johnson last testified before the subcommittee in 2018. Welcome back, Mr. Johnson.

Our second witness is Mr. Billy Bob Brown, Jr., executive assistant director of the Emergency Cybersecurity and Infrastructure Security Agency. This is Mr. Brown's first appearance before the subcommittee. Welcome, Mr. Brown.

Our third and final witness is Mr. Edward Parkinson, chief executive director of FirstNet Authority. Prior to joining FirstNet, Mr. Parkinson served as a professional staff member for 5 years on this subcommittee. Welcome back, Mr. Parkinson.

Without objection, the witnesses' full statements will be inserted in the record. I now ask each witness to summarize their statement for 5 minutes beginning with Director Johnson.

**STATEMENT OF ANTWANE JOHNSON, DIRECTOR, INTEGRATED PUBLIC ALERT AND WARNING SYSTEM, FEDERAL EMERGENCY MANAGEMENT AGENCY**

Mr. JOHNSON. Good morning, Chairwoman Demings, Ranking Member Cammack, and Members of the subcommittee. My name is Antwane Johnson and I am the director of the Integrated Public Alert and Warning System Program. I appreciate the opportunity to speak to you today about this program and how more than 1,600 agencies across the country are using it to save lives. An effective, timely, and far-reaching public alert and warning system is critical to communicating threats to public safety and providing people with guidance during times of crisis. IPAWS was created to provide the President with the means to reach the public under all conditions and to enhance and extend the National infrastructure to Federal, State, local, Tribal, and territorial officials for public alert and warning.

There are two main system components. First, the National Public Warning System supports warnings and emergency communications from the President or FEMA administrator in the event of a catastrophic or National emergency. It provides reach to approximately 90 percent of the U.S. population.

Second, the IPAWS Program also operates and maintains the IPAWS Open Platform for Emergency Networks, also known as IPAWS–OPEN. That provides Federal, State, local, Tribal, and territorial governments with the capability to send emergency alerts, warnings, and information to mobile devices, radio and television stations, NOAA Weather Radio, digital signboards and over 100 other internet-connected services.

Since the inception of IPAWS in 2011, more than 4 million lifesaving alert messages have been processed using IPAWS–OPEN. In June 2019, there were 1,200 local alerting authorities across the Nation who could alert and warn approximately 70 percent of the public. As of October of this year, 3 Federal agencies, all 50 States, 2 territories, 8 Tribal governments, and thousands of local alerting authorities utilized IPAWS services. Today, more than 87 percent of the U.S. population is covered by a local alerting authority and 100 percent of a population is covered by a State-level alerting authority.

In 2020, approximately 42,000 messages were issued each month by alerting authorities, of which 43 percent of wireless emergency alerts and 24 percent of emergency alert system alerts were initiated with both Spanish and English content. Pursuant to the PROTECT Act of 2003, the America's Missing: Broadcast Emergency Response Program, also known as AMBER, was developed in coordination with the National Center for Missing and Exploited Children, which is responsible for AMBER plans and allows au-

thorities to immediately distribute information about recent child abductions. As of October of this year, 94 children across the country have been safely returned to their families as a direct result of WEA information and community engagement.

Our IPAWS team also works closely with the U.S. Department of Justice Tribal Access Program for National Crime Information Officers and Tribal Law Enforcement agency members, as well as the United States Attorney's Office for Missing and Murdered Indigenous Persons to assist Tribal governments with developing alert and warning plans. Law enforcement agencies use IPAWS to issue Blue Alerts. These alerts provide rapid dissemination of information to law enforcement agencies, media outlets, and the public to aid in the apprehension of violent criminals who have killed or seriously injured an officer in the line of duty.

COVID–19 has also sparked a creative use by State and local alerting authorities. From March of last year through August of this year, 656 COVID–19-related alerts were sent by IPAWS. For example, Manatee County Public Safety Department used IPAWS for the first time to inform the public about local COVID–19 restrictions and the Navajo Nation was the first Tribal nation to send a COVID–19 alert through IPAWS.

IPAWS was used before, during, and after most severe weather events and 49 WEAs have been sent for wildfires in western States this year. Prior to Hurricane Ida's landfall, the National Weather Service, State and local, Tribal and territorial alerting authorities issued a series of timely WEA and EAS messages advising the public to take protective measures. After the storm passed, IPAWS remained a lifeline to New Orleans' residents helping them to find shelter and resources to aid during the recovery process.

To help our partners improve their ability to utilize IPAWS services, we conduct regular outreach by webinars, social media, and conducted our first National conference in September. We also revamped our on-line independent work-study courses offered through the Emergency Management Institute.

We will continue to promote adoption and use of IPAWS by emergency management and public safety officials. I thank you for your interest in the program and we look forward to collaborating with the subcommittee on ways to improve. I am happy to take any questions the subcommittee may have.

[The prepared statement of Mr. Johnson follows:]

PREPARED STATEMENT OF ANTWANE JOHNSON

NOVEMBER 2, 2021

INTRODUCTION

Good morning Chairwoman Demings, Ranking Member Cammack, and Members of the subcommittee. My name is Antwane Johnson, and I am the director of the Integrated Public Alert and Warning System (IPAWS) Program within National Continuity Programs (NCP), Office of Resilience at the Federal Emergency Management Agency (FEMA). I appreciate the opportunity to speak to you today about this program, and how more than 1,600 agencies across the country are using it to save lives.

WHAT IS IPAWS?

An effective, timely, and far-reaching public alert and warning system is critical to communicating threats to public safety and providing people with guidance during times of crisis.

Executive Order 13407 and The IPAWS Modernization Act of 2015 define FEMA's responsibility to provide a public alert and warning system. Section 706 of the Communications Act of 1934 requires Presidential access to commercial communications during "a state of public peril or disaster or other National emergency." The Robert T. Stafford Disaster Relief and Emergency Assistance Act, Section 202 directs FEMA to provide technical assistance to State and local governments to ensure that timely and effective disaster warning is provided. The National Defense Authorization Acts of 2020 and 2021 included additional IPAWS requirements significantly increasing the role of the FEMA administrator for dissemination of National alerts, previously only authorized to be sent by the President. In accordance with these statutes, IPAWS was created to enhance and extend a National infrastructure and capability to Federal, State, local, Tribal, and territorial (FSLTT) officials for public alert and warning.

IPAWS is a National system for local alerting. There are two main system components:

(1) The IPAWS Program Office maintains the National Public Warning System to support warnings and emergency communications from the President or FEMA administrator in the event of a catastrophic or National emergency. The President and/or FEMA administrator can warn the American people by a broadcast from private-sector radio stations that partner with FEMA. These stations, called FEMA Primary Entry Point (PEP) radio stations, receive all-hazards resiliency improvements at radio transmitter sites and provide reach to approximately 90 percent of the U.S. population. Activation of the National Public Warning System (PEPs) triggers the activation of all other radio and television providers that participate in the Emergency Alert System (EAS) in accordance with Federal Communications Commission regulations.

(2) The IPAWS Program also operates and maintains the IPAWS Open Platform for Emergency Networks, or "IPAWS–OPEN", that provides FSLTT governments the capability to send emergency alerts, warnings, and information to people in the geographic area of their jurisdiction via Wireless Emergency Alerts (WEA) to mobile devices, EAS messages on radio and television, NOAA Weather Radio broadcasts, and a growing number of voluntary information providers connected by the internet. More than 1,600 agencies are able to use the IPAWS–OPEN capabilities to provide emergency information in response to threats to public safety such as those issued this year by multiple States and local alerting authorities for Hurricanes Henri and Ida, as well as the coronavirus (COVID–19) public health emergency, and the mass demonstrations and civil disturbances in major cities last year. Changes to the Federal Communications Commission's (FCC) regulations, as directed by The National Defense Authorization Act for 2021 Section 9201, Reliable Emergency Alert Distribution Improvement (READI Act), recently authorized the FEMA administrator to use WEA for National emergencies. The broadened use of WEA ensures warnings related to situations of, nation-state attacks, natural disasters, acts of terrorism, and other man-made disasters can be sent from a Federal authority to warn people and provide protective action guidance.

IPAWS ADOPTION

Since the inception of IPAWS in 2011, more than 4 million life-saving alert messages have been processed using IPAWS–OPEN. It is important to note that in June 2019, there were 1,200 local alerting authorities across the Nation who were authorized to utilize IPAWS services to alert and warn approximately 70 percent of the public within the United States. Realizing that all emergencies start locally, in that same year (2019) FEMA initiated the IPAWS "Close the Gap" campaign to increase the number of local alerting authorities. As a result of this initiative and stakeholder outreach, as of October 2021 3 Federal agencies, all 50 States, 2 territories, 8 Tribal governments and thousands of local alerting authorities utilize IPAWS services. Today more than 80 percent of the U.S. population is covered by a local alerting authority who has been authorized and trained to utilize IPAWS, and 100 percent of the population is covered by a State-level alerting authority.

In 2020, twice the number of agencies used IPAWS to send alerts as in 2019, resulting in a 182 percent increase in the number of alerts to the public by local alerting authorities in response to COVID–19, civil unrest, wildfires, AMBER alerts, and several other public safety threats. In 2020, 43 percent of WEAs and 24 percent of

EAS alerts sent via IPAWS were initiated with both Spanish and English message content, meaning that devices set with Spanish as the primary language choice would display the alert in Spanish. IPAWS works to expand its reach in accessible communications capabilities and services. IPAWS uses the Common Alerting Protocol, or CAP, which allows alerts sent through the system to transport rich multimedia attachments and links. By sending CAP-compliant messages through IPAWS, private industry partners are able to develop content or compatible devices that can facilitate receipt of emergency alerts by individuals with disabilities. The IPAWS Program Management Office (PMO) is diligently working toward integrating additional, accessible technologies and encouraging industry innovation to meet the needs of all people.

IPAWS ALERTS, WARNINGS AND NOTIFICATIONS

*IPAWS Use for AMBER Alerts*

In 2003, President George W. Bush signed the Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today (PROTECT) Act of 2003 (Public Law 108–21). This Act established the National coordination of State and local America's Missing: Broadcast Emergency Response (AMBER) programs. The National Center for Missing & Exploited Children (NCMEC) is responsible for AMBER plans, which allows broadcasters and transportation authorities to immediately distribute information about recent child abductions to the public and enables the entire community to assist in the search for and safe recovery of children.

The AMBER Alert program is a voluntary partnership among law enforcement agencies, broadcasters, transportation agencies, and the wireless industry to activate an urgent WEA. For example, on October 6, 2021 a 1-year-old boy was in the back seat of a car that was stolen from a grocery store parking lot in East Nashville, TN, while his parents were inside the store. The car was later abandoned with the child still in the back seat. A State-wide AMBER alert was issued via WEA, and a citizen recognized the vehicle from the information contained in the WEA message and notified law enforcement. The child was recovered safely.

As of October 2021, 94 children across the country have been safely returned to their families as a direct result of WEA information and community engagement.

Our IPAWS team works closely with the U.S. Department of Justice Tribal Access Program for National Crime Information officers and Tribal Law Enforcement agency members as well as the United States Attorney's Office for Missing and Murdered Indigenous Persons to assist Tribal governments with developing alert and warning plans. Currently, the Cocopah Tribe, Navajo Nation, Eastern Band of Cherokee Indians, and the Confederated Tribes of the Chehalis Reservation have access to IPAWS and can send geo-targeted Amber Alerts.

*IPAWS Use for Other Emergencies*

Public Safety Officials have expanded their use of IPAWS to include both public safety notifications and imminent threat alerts and warnings. This allows public safety officials to increase their reach to the public. Some examples include public safety notifications regarding 9–1–1 outages; boil water notices with respect to contamination; stay-at-home orders and COVID vaccination sites; missing and endangered persons, particularly for young adults that do not meet AMBER alert criteria; and missing and endangered elderly (commonly known as Silver Alert) and individuals with disabilities (commonly referred to as a Golden Alert).

Law enforcement agencies use IPAWS to issue Blue Alerts. These alerts provide rapid dissemination of information to law enforcement agencies, media outlets, and the public to aid in apprehension of violent criminals who have killed or seriously injured an officer in the line of duty. These alerts may also be issued when a suspect is considered a credible threat to law enforcement, or an officer is missing in the line of duty. As an example, the Texas Division of Emergency Management issued a Blue Alert via WEA after an officer was killed in the line of duty and authorities in Tampa, Florida issued a Blue Alert via WEA after a 26-year-old police officer was shot in the head in Daytona Beach. As a result, both suspects were quickly apprehended by law enforcement.

*IPAWS Use During COVID–19, Wildfires, and Recent Disasters*

COVID–19 sparked creative uses of IPAWS by State and local alerting authorities who leveraged IPAWS–OPEN capabilities to alert the public to rapid increases in COVID–19 infections, mandates, and vaccine information. IPAWS–OPEN usage from March 2020 through August 2021 included a total of 656 COVID–19-related alerts sent between WEA and EAS. The Manatee County Public Safety Department used IPAWS for the first time to inform the public about local COVID–19 restrictions and the Navajo Nation was the first Tribal nation to send a COVID–19 alert

through IPAWS. As an example, Governors in Maryland, Virginia, and Michigan used IPAWS to issue mandates and amplify guidance issued by the White House COVID–19 task force and the CDC, directing people to stay at home.

IPAWS was used before, during, and after the most severe weather on the West Coast. As of October 2021, there have been 49 WEAs sent for wildfires in 2021, and the unprecedented heat wave and severe drought on the West Coast has also prompted the need for alerts. Counties in California, Oregon, Nevada, Idaho, Texas, and Utah sent fire warnings and follow-up evacuations where warranted. In August 2021, the city of Portland, Oregon, and Multnomah County sent WEAs in both English and Spanish informing people of severe heat and the need to stay cool and check on other people. These have increased recognition of the need to ensure protective actions are taken before an event turns life-threatening.

Prior to Hurricane Ida at the end of August 2021, State, local, Tribal, and territorial alerting authorities issued a series of timely WEA and EAS alerts advising the public to take protective measures. The New Orleans Office of Homeland Security & Emergency Preparedness as well as local Alerting Authorities sent more than 200 alerts that aided the safe evacuation, shelter, and support of residents. The Louisiana Governor's Office issued IPAWS alerts on behalf of counties that were unable to issue an alert. After the storm passed and hundreds of thousands of people were without power, IPAWS remained a lifeline to New Orleans residents, helping them find shelter and resources to aid during the recovery process.

The 77 National Primary Warning System (NPWS) PEP stations continue to serve as a critical communications lifeline for news and updates before, during, and after powerful storms such as Hurricane Ida, which left the New Orleans area with no power or television and spotty cell service. New Orleans radio station WWL is known among locals as the "hurricane station" through its use of the PEP station there, equipped with FEMA-owned back-up equipment and generators. Nineteen station employees provided around-the-clock coverage to provide updates and support for the New Orleans community.

As of October 2021, State and local authorities, and the National Weather Service (NWS) have sent nearly 800 WEAs during the 2021 hurricane season. For the two most significant storms impacting the United States in the 2021 season, Henri and Ida, State and local authorities and the NWS sent nearly 400 emergency messages through IPAWS.

### IPAWS IN RECENT NATIONAL DEFENSE AUTHORIZATION ACTS (NDAAS)

Public Law 116–92 (NDAA fiscal year 2020) was signed into law in December 2019 and included Section 1756, Integrated Public Alert and Warning System. This provision included 33 new and additional requirements for the IPAWS program that support users and the development of tools to warn and educate the public about emergency alerting and protective action guidance to take when they receive an alert. FEMA is reviewing the NDAA requirements and prioritizing resources as appropriate.

The National Defense Authorization Act for 2021 Section 9201, Reliable Emergency Alert Distribution Improvement (READI Act) directed the FCC to adopt regulations to ensure that mobile devices cannot opt out of receiving WEA alerts from the FEMA administrator, encourage chief executives of States to form State Emergency Communications Committees (SECCs), establish a State EAS plan checklist for SECCs, amend requirements for SECCs, ensure SECCs meet, review, and update their EAS plans annually, enable the FEMA administrator, State, local, Tribal, and territorial governments to report false EAS and WEA alerts, and provide for repeating EAS alerts for emergency warnings issued by the President, the FEMA administrator, and any other entity determined appropriate by the Commission, in consultation with the FEMA administrator. FEMA commends the FCC for quickly acting to change the WEA alert category "Presidential" to "National" and authorizing the FEMA administrator's use of the National Emergency Message category to send a WEA Nation-wide should we experience an imminent threat of National consequence.

### THE IPAWS TECHNICAL SUPPORT SERVICES FACILITY

In response to the National Advisory Council's Recommendation and NDAA 2020 direction to improve the IPAWS lab, the IPAWS PMO significantly increased the capabilities of the lab and stood up the IPAWS Technical Support Services Facility in October 2020.

The new 24/7 Technical Support Services consist of a contract staff of 18 subject-matter experts, providing around-the-clock support services to all FSLTT emergency management agencies in their use of IPAWS. The facility provides alerting authori-

ties with test and evaluation, operational assessments, IPAWS demonstrations, and expert technical support. The facility also provides an interactive and closed IPAWS testing environment and allows users the opportunity to practice and train to increase familiarity and confidence using IPAWS.

The facility has supported 268 calls from Federal, State, Tribal, and territorial agencies between January–October 2021 as well as calls from the public who have questions about alerts in their area.

### IPAWS–OPEN AND NPWS MODERNIZATION

FEMA continues sustaining and enhancing IPAWS systems and infrastructure, including IPAWS–OPEN modernization and migration to a cloud infrastructure environment, as well as modernization of NPWS legacy PEP stations.

In April 2021, FEMA transitioned IPAWS–OPEN from Department of Homeland Security data centers into Amazon Web Services GovCloud environment to increase system availability and reliability of greater than 99.9 percent. This improvement in services provides reasonable assurances that IPAWS–OPEN services experiences no more than 56 minutes of system down time, (inclusive of maintenance) for the year and the successful processing of approximately 42,000 messages per month.

FEMA has completed modernization of 13 of the original group of PEP stations since 2019, increasing the percentage of the U.S. population covered by a FEMA connected radio station with High Altitude Electromagnetic Pulse (EMP) protection to 51 percent. On October 15, 2021, WBZ radio station in Boston, MA became the 13th station modernized station to receive the full complement of resilient transmitter, generation, and fuel-system capabilities and EMP protections. In May 2021, IPAWS PEP equipment underwent EMP testing at the Department of Defense's test range at the Patuxent Naval Air Station. The IPAWS PEP equipment underwent 36 full power pulses, double the 16 planned pulses without failure or degradation of system capabilities. This addresses the mandate that our critical infrastructure systems be mission ready and capable of operating before, during, and after an EMP event.

### STAKEHOLDER ENGAGEMENT

As of October 2021, FEMA has conducted 23 IPAWS webinars this year with average attendance of 151 live participants and 12,611 downloads of webinar content and issued 35 social media posts with more than 41,000 views and nearly 1,300 connections.

The program also revamped its on-line independent study courses offered through the FEMA Emergency Management Institute. As of mid-year, 717 people completed the required IS–247 "IPAWS for Alert Originators" course on-line and 227 people completed the IS–250 on-line course "IPAWS for Alerting Authorities." This training provides skills to draft authenticated, effective, and accessible warning messages, and best practices in effective use of the Common Alerting Protocol. It is mandatory for establishing new Alerting Authorities.

The program also distributes a "Monthly Tip" to all Alerting Authorities and Vendors. These Tips, sent via email to more than 6,000 stakeholders, provide guidance and insight related to using IPAWS.

We hosted the first-ever virtual IPAWS Users Conference on September 15. This 6-hour event targeted current IPAWS Alerting Authorities and Vendors and over 500 people registered.

### IPAWS PROGRAM GOALS AND CHALLENGES

The IPAWS program office has been engaging vendors of IPAWS-compatible software to encourage better integration of IPAWS screens for consistency and creation of effective public alert and warning messages.

We will continue to promote adoption and use of IPAWS by emergency management and public safety officials. Through the IPAWS Stakeholder Engagement and Customer Support teams, the program office works with State, local, Tribal, and territorial officials to promote use of the system. We also provide information and support on various Federal grant programs that may provide funding for alerting authorities to purchase alerting software that interfaces with IPAWS.

IPAWS will also continue to make local and State emergency managers aware of the IPAWS Technical Support Services Facility.

In accordance with new WEA rules established by the FCC in 2021, FEMA is working with wireless carriers and alerting software vendors to enhance WEA capabilities to support the enhanced role of the FEMA administrator and the Commission's future actions to address enhancements to the Emergency Alert System.

CONCLUSION

Every day I am grateful for the opportunity to work with a program dedicated to helping alert and provide guidance to people during times of crisis. Thank you for your interest in the program and we look forward to collaborating with this subcommittee on ways to improve. I am happy to take any questions you have at this time.

Mrs. DEMINGS. Thank you so much, Mr. Johnson, for your opening statement. I now recognize Director Brown to summarize his statement for 5 minutes.

**STATEMENT OF BILLY BOB BROWN, JR., EXECUTIVE ASSISTANT DIRECTOR, EMERGENCY COMMUNICATIONS, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY**

Mr. BROWN. Thank you, Chairwoman Demings, Ranking Member Cammack, and Members of the subcommittee. It is a pleasure to be with you here today to discuss the Department of Homeland Security Cybersecurity and Infrastructure Security Agency, or CISA's, efforts in enhancing the Nation's interoperable emergency communications capabilities. But it is not just CISA. It is a partnership.

SAFECOM is a partnership of more than 35 public safety associations and emergency responders. It established our guiding principle that interoperability is not just about technology, but about people working together. According to SAFECOM, 20 percent of the interoperability challenge is related to technology. Eighty percent is related to people.

The 21st Century Emergency Communications Act of 2006 established a Nation-wide focus on interoperability as a response to communications challenges experienced during both September 11 and Hurricane Katrina. Great strides have been made in improving public safety communications and information management technologies since that time.

Digital land mobile radio and broadband technologies are accelerating dissemination of critical information, while Next Generation 9–1–1 will enable public safety entities to provide optimal service to their communities and when requested, to neighboring communities in need of additional resources or assistance. However, the threat landscape has also evolved with newer challenges posed by more frequent and extreme weather events, cyber attacks, and the global pandemic.

CISA is positioned to help our stakeholders and partners reduce risk by focusing on three areas. First, interoperability, second, collaborative planning, and third, expanding the priority service capability.

First, we promote interoperability and resilience by providing the tools and resources for stakeholders to operate in the next generation environment and cyber ecosystem, including direct assistance to jurisdictions across the United States improving awareness of Next Gen 9–1–1 capabilities.

Second, we continue to bolster our existing partnerships and are building bridges to emergency communications stakeholders across critical infrastructure sectors to reduce risk to the National critical functions. CISA in partnership with SAFECOM and the National Council of State-wide Interoperability Coordinators provides resources to the District, States, territories, and Tribal nations to de-

velop State-wide communications interoperability plans. These plans advocate sustainment and investment funding from State and local governments.

Finally, we are partnering with industry and research organizations to make priority data, video, and information services available to all National security and emergency preparedness stakeholders through a constellation of carrier partners. CISA ensures that interoperable priority service requirements are satisfied by cooperating network service providers as they evolve to Next Generation networks. Promoting the awareness of these services and the use thereof, is key because when sharing information, every second counts.

I am encouraged by the progress made since 9/11, and am proud of the contributions made by our community of stakeholders. But I am also aware of the fiscal and technological challenges that remain, as well as the scarcity of resources.

Additionally, unchecked competitiveness and siloed thinking is another threat that our adversaries exploit. They seek to divide and conquer. Our partnerships, CISA's technical expertise, and your leadership ensure the safety of our communities and first responders. Together we can wisely integrate Next Generation capabilities and maintain a steadfast focus on the people who are using these capabilities to protect the homeland. Thank you and I look forward to your questions.

[The prepared statement of Mr. Brown follows:]

PREPARED STATEMENT OF BILLY BOB BROWN, JR.

NOVEMBER 2, 2021

Thank you, Chairwoman Demings, Ranking Member Cammack, and esteemed Members of the subcommittee. It is a pleasure to be here with you today to discuss the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency's (CISA) efforts in enhancing the Nation's interoperable emergency communications capabilities.

Since DHS last appeared before this subcommittee in 2017, the communication and information management technologies used by the Nation's public safety community has evolved and advanced dramatically, including video, data, internet protocol (IP), and broadband communications. The risk landscape has also become more challenging with more frequent and extreme weather events, cyber attacks, and the severe impacts of a global pandemic. As Members heard during the October 7 hearing: The threats also come in the form of aging infrastructure (for Land Mobile Radio [LMR] systems, 9–1–1 centers, etc.) and a lack of dedicated funding for personnel, equipment, and other communications resources.

The Cybersecurity and Infrastructure Security Agency Act of 2018 established CISA to protect the Nation's critical infrastructure from physical and cyber threats. At the nexus of physical and cyber threats lie emergency communications. Our division—previously known as the Office of Emergency Communications (OEC) and now as the CISA Emergency Communications Division (ECD)—was created by Congress in response to the communications challenges experienced during Hurricane Katrina in 2005 and the terrorist attacks of September 11, 2001. We believe the best defense against threats to operable and interoperable emergency communications is integrated, collaborative planning for strong governance, standard operating procedures, training & exercises, and technology solutions. In other words, solutions for effective interoperable emergency communications is more about people, partnerships, and practices, and to a lesser extent about the technology. CISA is positioned to assist our stakeholders and partners in addressing current and future threats to interoperable communications even as technologies evolve.

*Working at the National Level*

Leading from a stakeholder-driven approach is at the heart of CISA's mission. We engage the people who are doing this work every day to build guidance for the Nation's National security and public safety communications community, a community which includes organizations at all levels of Government and across all disciplines.

CISA is the executive agent of SAFECOM, a public safety advisory board which aims to improve multi-jurisdictional and intergovernmental communications interoperability. SAFECOM works with CISA and key emergency response stakeholders and all public safety disciplines to improve communications interoperability for all emergency response providers across Federal, State, local, Tribal, and territorial governments, and international borders. CISA also works closely with the National Council of State-wide Interoperability Coordinators (NCSWIC), comprised of State leaders from the 56 States and territories. SAFECOM and NCSWIC develop and release guidance documents, tools, and resources and facilitate the implementation of these tools to support the public safety community and improve communications resilience and interoperability. Additionally, CISA maintains a close relationship with Federal partners that make up the Emergency Communications Preparedness Center (ECPC), which includes 14 Federal departments and agencies, and with the First Responder Network Authority (FirstNet Authority).

These partnerships, resources, and efforts over the decades were critical in mitigating and stemming the communications impacts brought on by the global pandemic (e.g., tele-health, tele-medicine, alternate care facilities, the need for additional bandwidth for research and operations).

*National Planning*

Title XVIII of the Homeland Security Act of 2002, as amended, requires that CISA develop a National Emergency Communications Plan (NECP). The purpose of the NECP is to implement a whole-of-Nation approach to achieving emergency communications interoperability. The NECP's goals and initiatives are informed by the SAFECOM Nation-wide Survey (SNS), which is a Nation-wide effort to obtain actionable and critical data to inform the Nation's emergency communication policies, programs, and funding. Additionally, SNS results are used to complete the Nationwide Communications Baseline Assessment (NCBA), a Congressionally-mandated assessment of Federal, State, local, Tribal, and territorial governments, focusing on analyzing the current state of emergency communications capabilities, identifying Nation-wide gaps, and measuring the evolution of emergency communications since the last assessment. CISA's last released the updated NECP in September 2019.

In 2018, CISA, through the SNS, surveyed thousands of local public safety organizations about their emergency communications. While the majority of agencies reported their emergency, communications capabilities had improved over the past 5 years, the survey also indicated:

- Approximately half of the public safety organizations reported their LMR systems are more than 10 years old.
- 76 percent of public safety organizations have no or insufficient funding for capital investments in emergency communications network systems.
- Less than one-quarter of all the agencies reported having sufficient cybersecurity funding.
- Seven percent of the agencies are sharing biometric data with other organizations, while over 50 percent are sharing GIS data.

*State-wide and Tribal Planning*

Through the Interoperable Communications Technical Assistance Program (ICTAP), CISA provides all States and territories with direct support in the form of State-wide planning workshops and technical assistance (TA) training, tools, and resources. Since 2008, more than 2,550 TAs have been delivered to all States and territories. As the technology used by public safety has evolved, so have the offerings. For example, the Communications Unit (COMU) program, which outlines the functions, positions, training, and certifications required to support interoperable incident communications, has been updated. It now includes an Information Technology Service Unit Leader position and course to assist incident command in managing the confluence of voice, video, and data communications and information, cybersecurity, and application management for incident planning and response. To date, more than 17,000 personnel have been trained to fill COMU positions.

State-wide Communication Interoperability Plans (SCIPs) play the crucial role of enabling States and territories to align and prioritize their communications needs and advocate for funding to their local and State governments. SCIPs are generated

via State-wide planning workshops. This process of meeting and planning to create alignment allows for the development of key relationships before an incident occurs.

In 2001, there were no State-wide plans for interoperable communications. Twenty years later, every State and territory has a SCIP that is regularly updated to address needs involving governance, training, technology planning, funding sustainability, and cybersecurity. CISA is committed to helping States regularly improve these plans.

*Communications Resiliency*

CISA administers services that enable the end-to-end movement of information with priority when networks are congested or degraded. The Government Emergency Telecommunications Service (GETS) provides priority for landline communications by leveraging commercial networks. The Wireless Priority Service (WPS) is a model public-private partnership: CISA administers contracts with all major National and regional commercial carriers to provide prioritized access for users in and across wireless networks. Telecommunications Service Priority (TSP) is the third CISA-administered service, enabling prioritized provisioning and restoration of priority services for organizations that have a National security mission. While CISA manages these priority services programs, the Federal Communications Commission's rules govern some aspects of TSP and WPS. The Commission has proposed to update its rules to reflect today's marketplace and governance framework and to authorize the prioritization of next-generation services and technologies. CISA supports many of the proposed rule changes.

We are in the final stages of Phase 1—Next Generation Network Priority Services (NGN–PS), which will provide prioritized access for Voice over Internet Protocol (VoIP). Phase 2 focuses on the movement of data, video, and information services (DV&IS) with priority, which is mission-critical in the face of evolving threats and response capabilities.

Working with our industry partners, we are proud to offer these services at no cost to our stakeholders. These services provide resilience in ways that all local, State, Tribal, territorial, and Federal users can use, and have proved critical in maintaining communications at the State, local, Tribal, and territorial (SLTT) level during natural disasters. There is no patchwork of "have and have nots" when it comes to the affordability of resilient communications.

*Field Coordination*

Since OEC was established in 2007, we have adapted to better serve our stakeholders. We went from having a centralized to a regionalized posture to meet stakeholders in the field. This effort started in 2010 with the establishment of the Regional Coordination Program. CISA now has 16 full-time experts in the field. CISA Emergency Communications Coordinators (ECCs) serve as key partners in coordinating communications and communications restoration before, during, and in response to natural disasters, pandemic response and large, planned events (e.g., Super Bowls, Presidential inaugurations). These coordinators build trusted relationships with and across the public safety community and Government partners to establish strong governance, plan for technology insertion, and identify sustainable funding sources.

CISA has deployed ECCs to support emergency communications coordination and power restoration during numerous natural disasters (e.g., hurricanes, wildfires, pandemic) and incidents (e.g., State cybersecurity incidents) over the years. The ECCs work directly with the NSWIC to provide on-site support to States and jurisdictions and situational awareness to CISA leadership. CISA staff members also provide Emergency Support Function No. 2 (ESF–2) desk support at the National Response Coordination Center to ensure Federal communications needs are supported. Emergency activations and provisioning of priority telecommunications (i.e., GETS, WPS, TSP) are also provided to mitigate network congestion for Federal partners, SLTT public safety officials, major hospitals, critical infrastructure manufacturers, and wireless & wireline service providers.

SUPPORTING INTEROPERABLE EMERGENCY COMMUNICATIONS INTO THE FUTURE

As stated in our last statement to the subcommittee in 2017, the emergency communications ecosystem previously consisted of a citizen calling a PSAP for help, a call operator radioing the information to fire or police, and public safety officials and responders speaking to each other on LMR. However, new technologies have drastically changed the emergency communications ecosystem, not only transforming how citizens talk to each other, but also how public safety works together and engages with citizens. These new technologies bring increased capability but will require continued and increased support to our partners through training, technical

assistance, and best practices as LMR remains a critical communications tool, along with these new capabilities for public safety.

CISA counters the evolving threats to emergency communications by focusing its initiatives in three priority areas:

1. Emergency Communications Interoperability: Promoting operability, resilience, and interoperability by providing the tools and resources for stakeholders to operate in the next generation environment and cyber ecosystem.
2. Integrated, collaborative communications planning: Bolstering and building teams and communities of practice with public safety stakeholders and communicators across all parts of the Federal and SLTT (FSLTT) and critical infrastructure sectors.
3. Priority services adoption: Partnering with industry and research organizations to make priority DV&IS available to all stakeholders with national security missions.

*Emergency Communications Interoperability*

*Integrating LMR and Broadband Communications*.—Although LMR remains essential in emergency communications, the benefits and opportunities broadband offers to public safety are undeniable. Citizens will be able to send a picture of a suspicious package or videos of an event as it is happening to PSAPs that can then share those files with first responders. This capability accelerates the provision of critical information to determine how to respond and what resources will be needed. These advancements are tied to the progress toward implementing the newest tool in the emergency communications toolbox. LMR will continue to be a primary method of communication for first responders as broadband continues to greatly improve interoperable communications across the country.

*Public Safety Transition to Next Generation–911 (NG–911)*.—The transition to NG–911 is an effort to move PSAPs across the country from the analog systems used since before 9/11 to a digital or IP-based 9–1–1 system. CISA will provide direct assistance to jurisdictions across the United States to implement NG 9–1–1 capabilities and ensure cybersecurity interconnectivity and interoperability amongst those systems using common standards Nation-wide. Among the benefits of Nationwide interoperability are the ability to respond to 9–1–1 requests faster and with greater accuracy, greater situational awareness, greater resilience, and with more consistent quality. It will enable first responders, emergency management, and other public safety entities to provide optimal service not only to their own communities, but also to neighboring communities in need of additional resources or assistance. Furthermore, interconnectivity and interoperability among 9–1–1 systems positions the Nation to obtain better awareness of community needs, identify trends, and evaluate how effectively U.S. residents and visitors are served.

*Cybersecurity in Emergency Communications*.—The technologies that have made the Nation's emergency communication more efficient have also exposed it to the risks and vulnerabilities inherent in information technology and operational technology. As emergency communications transitions from voice-only to DV&IS, emergency communicators must defend against attacks from adversaries seeking to interfere and profit. To do so, CISA is improving its cybersecurity capabilities to counter threats, mitigate critical vulnerabilities, and manage incidents, as well as help organizations build resilience, design technology securely, and manage risk before cyber incidents occur. Specifically, CISA is working to:

- Share cybersecurity information, analyze cybersecurity threats and vulnerabilities, and issue guidance and best practices to detect and prevent cyber intrusions into emergency communications networks, including Next Generation 9–1–1.
- Adapt governance models to incorporate cybersecurity planning and intrusion prevention.
- Customize cyber-focused Technical Assistance for Public Safety Emergency Communications Centers, 9–1–1 Systems and LMR functions to mitigate ransomware/Telephony Denial of Service (TDoS) attacks on public safety networks, and systems that affect 9–1–1 and emergency communications.
- Shape cybersecurity initiatives (secure mobile, etc.) that include Advanced Encryption Standard (AES) for Federal voice networks and CISA-hosted interoperability grant programs for both voice and DV&IS capabilities.
- Refine interoperability and NG 9–1–1 risk profiles; and
- Customize assessment tools into a user-friendly software assessment for CISA COMU specialists and Cybersecurity Advisors (CSAs).

*Integrated, collaborative communications planning*

*Advancing Interoperability in Federal Agencies, Tribal, and International Communities (One DHS, ECPC, Tribal Engagement).*—To ensure both horizontal and vertical emergency communications interoperability, CISA's support must continue to extend beyond its current SLTT stakeholders and proactively engage in interoperability advancement activities for Federal Agencies, Tribal Nations, and International communities. CISA will proactively engage in technical advisement, standards promotion, and advocacy activities to guide interoperability planning for these stakeholder groups. CISA seeks to:

- Extend outreach and technical assistance for rural communities and other underserved public safety entities.
- Build cybersecurity expertise in public safety emergency communications.

*Bolster and Build communities for emergency communications interoperability planning*.—Integrated, collaborative communications planning is the center of gravity in CISA's work with the public safety community. We will continue to bolster our relationships with partners at all FSLTT levels. At the same time, this model of trusted partnerships sets the example of what CISA ultimately aims to achieve across all 16 critical infrastructure (CI) sectors. The focus will be on building teams and communities of practice that can offer lessons learned and resources to others in the community so that everyone benefits from working together. To that effect, CISA seeks to:

- Engage CI Sectors by extending emergency communications interoperability assistance and outreach to some of the ~4,000 critical infrastructure sector entities with ties to National security and emergency preparedness.
- Champion local/regional-level relationship-building with stakeholders.

*Priority services adoption*

*Priority Services Awareness and Adoption and Priority Services Next Generation Phase II*.—CISA ensures that priority communications requirements are satisfied as service providers evolve to next generation networks that employ emerging technologies. Promoting the awareness of these services and the use thereof is as important as the technological investment in evolving these services.

*Priority Services Awareness and Adoption*.—Engage in strategic communications and outreach activities with stakeholders to increase awareness, enrollment, and usage of services.

*NGN–PS Phase 2*.—NGN–PS is a multi-phase, technology insertion that will ultimately deliver priority for voice and data communication services. The Phase 2 DV&IS Program moves beyond Phase 1 (voice) and will provide priority for DV&IS over the IP networks. Phase 2 will acquire DV&IS priority capabilities through several major service providers, including cellular and cable networks. Additionally, Phase 2 includes proofs of concept for critical components necessary to achieve cybersecurity assurance for priority across multiple networks, provides end-to-end priority, and develops requirements for priority over Wi-Fi.

CONCLUSION

Thank you, Chairwoman Demings, Ranking Member Cammack, and Members of this subcommittee for the opportunity to provide this overview and update with you today. The Nation's public safety agencies protect the homeland, and they rely on resilient, interoperable communication systems to carry out their mission and protect our Nation. While we have made tremendous strides in building interoperable emergency communications capabilities through close coordination with the National security and public safety community, the work must continue and evolve. As the technologies continue to advance, so does the threat landscape. CISA has and will continue to serve as a trusted partner to help public safety officials defend against threats and build their capabilities for the future. With your continued support, we know we can help our partners and stakeholders prepare for the future of emergency communications and wisely integrate next generation capabilities while always maintaining a focus on the people who are using these capabilities as they protect the homeland. We are stronger together. I look forward to our discussion this morning, and I am pleased to answer any questions you may have.

Mrs. DEMINGS. Thank you so much, Director Brown, for your testimony. I now recognize Mr. Parkinson to summarize his statement for 5 minutes.

**STATEMENT OF EDWARD PARKINSON, CHIEF EXECUTIVE OFFICER, FIRST RESPONDER NETWORK AUTHORITY, NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION**

Mr. PARKINSON. Thank you very much, ma'am, and good morning to yourself, Ranking Member Cammack, and all subcommittee Members. I appreciate the opportunity to being here today to provide an update on the status of the First Responder Network Authority and the progress that we have made along with our contracting partner to deploy the Nation-wide interoperable public safety broadband network. My name is Edward Parkinson and I am the CEO of the Authority and again, thank you very much, ma'am, for the shout-out to my alumni status in front of this subcommittee. I know there are some—it is strange being on this side of the camera having been on behind the dais, especially when Mr. Johnson and Billy Bob's predecessors were there. So, it is good to see a lot of familiar faces.

I will submit my opening statement for the record, of course. But really just the initial idea of the First Responder Network Authority and was rooted in the 9/11 Commission Report. With this recommendation, public safety tirelessly advocated in front of the committee, in front of the whole of Congress, and ultimately a bipartisan agreement, bicameral agreement was reached to allocate dedicated spectrum to public safety. The result was the creation of FirstNet.

Since we were created, the FirstNet Authority has been focused on the Congressionally-mandated mission to deploy public safety's network. This isn't our network. This isn't the Authority's network. This is public safety's. FirstNet is trusted by over 18,5000 agencies. Over 2.8 million public safety connections are now leveraging FirstNet. All of these numbers were zero just at the beginning of 2018.

We know that behind those numbers are our Nation's heroes running toward danger 24/7, 365. There are paramedics using GPS to find the fastest route to a stroke victim's home. Firefighters, such as Representative Cammack's spouse, utilizing first responders and FirstNet's deployable trucks to connect to the network as they battle wildfires out west and, indeed, hurricane response and many other disasters around the country. There are law enforcement officers at county fairs and marathons receiving text messages with a photo of a missing child and being able to now deliver that to their peers to hopefully find those children safe. We have got numerous examples of that taking place.

FirstNet was also successfully leveraged to support D.C. first responders during the Capitol riots on January 6. It is proven that dedicated spectrum works. This type of dedicated service did not exist prior to FirstNet. We at the Authority engage extensively with public safety to understand their needs, to inform future investments into the network. In fiscal year 2020, my team conducted over 1,200 engagements with public safety in every single State, territory, and the District of Columbia with all public safety disciplines. We are lucky to have a board, including Representative Billy Bob Brown, who represents the Secretary of Homeland Security, as well as private and public safety experts. Our Public Safety

Advisory Committee, PSAC, our new chair, in fact, Chris Lombard testified at the first of these two hearings just a few weeks ago. Based on public safety's feedback, the Authority's first set of network investments expanded our fleet of deployable assets, which are used by first responders at zero additional cost. We began upgrading our core for initial 5G capabilities. These investments reflect our dual focus on better service and providing 5G capabilities on the network, which is visible today in numerous markets.

Now, there are two issues I would like to particularly highlight for the committee. The first is the renewal of the First Responder Network Authority's Band 14 spectrum license. The second is the reauthorization of our program. The Bank 14 spectrum license is crucial to providing dedicated communications for first responders. Our enabling statute back in 2012, only instructed the FCC to initial—to license an initial 10-year license. The statute requires that we, the Authority, apply for and the FCC to decide on next year whether or not to renew this license. This spectrum issue is linked to reauthorization. Next February, the GAO, as required by the Act, will present their recommendations to Congress regarding the FirstNet's 15-year sunset provision, which is slated to go into effect in 2027. I look forward to working with the FCC on license, as well as this committee and all of Congress on the details of the GAO recommendations and our spectrum renewal.

I ask the subcommittee to continue to support the Authority and, indeed, entire program as we enter the next phase of this program to innovate and invest in public safety's network. The support of Congress is crucial to FirstNet and in turn, public safety's success. This is not, as I mentioned before, our system, this is public safety's. The public safety community fought long and hard for the creation of FirstNet and it is up to us to continue to strive to achieve their vision. Thank you very much for the time. I look forward to the questions as well.

[The prepared statement of Mr. Parkinson follows:]

PREPARED STATEMENT OF EDWARD PARKINSON

NOVEMBER 2, 2021

Chairwoman Demings, Ranking Member Cammack, and all subcommittee Members, I would like to thank you for the opportunity to appear here today to provide an update on the First Responder Network Authority (FirstNet Authority) and the deployment of the Nation-wide, interoperable public safety broadband network (NPSBN, Network, or FirstNet). My name is Edward Parkinson, and I am the executive director of the FirstNet Authority. I am also a proud alumnus of the House Homeland Security Committee. Having worked for 5 years as a professional staff member for the committee, I have a great appreciation for the important work the committee does every day.

I'd also like to recognize my colleagues on the panel, executive assistant director Billy Bob Brown, Jr. with the Cybersecurity and Infrastructure Security Agency (CISA), Emergency Communications Division, and (acting) deputy assistant administrator, Antwane Johnson, with the Department of Homeland Security's Integrated Public Alert and Warning System (IPAWS). I appreciate the work that CISA and IPAWS have done to improve emergency communications in the United States, and personally appreciate Executive Assistant Director Brown for his work as the Department of Homeland Security's designee to the FirstNet Authority Board.[1]

Today's hearing aims to examine emergency communications 20 years after September 11, 2001. While many challenges certainly remain, I believe that the

[1] See FirstNet Authority, FirstNet Authority Board: *https://firstnet.gov/about/leadership/billy-bob-brown-jr.*

FirstNet Authority has enhanced the Nation's emergency communications, and thus has made Americans safer and more secure.

9/11 COMMISSION REPORT AND PUBLIC SAFETY'S NEED FOR DEDICATED SPECTRUM

FirstNet was derived from the tragedy of 9/11—the initial idea for a Nation-wide public safety "communications" network is rooted in the recommendations of the 9/11 Commission Report.[2] In their July 2004 report, the 9/11 Commission recommended that Congress support the allocation of dedicated radio spectrum for public safety:

"Recommendation: Congress should support pending legislation which provides for the expedited and increased assignment of radio spectrum for public safety purposes . . . ."[3]

With this recommendation and the support from first responders and the public safety community across the country, the FirstNet Authority was eventually established by Congress, with this very committee taking a lead in the development of the Middle Class Tax Relief and Job Creation Act of 2012 (Pub. L. 112–96) (Spectrum Act).[4] Public safety is forever indebted to Congress for the bipartisan support that this legislation enjoyed in fulfilling the 9/11 Commission Report's recommendation and allocating 20 MHz of dedicated spectrum to public safety.

FIRSTNET TODAY AND INTO THE FUTURE: AN OPERATIONAL AND EXPANDING NETWORK INCREASINGLY RELIED ON BY PUBLIC SAFETY

Since the passage of the Spectrum Act, the FirstNet Authority has been solely focused on our Congressionally-mandated mission of deploying public safety's Nationwide, interoperable broadband network.

The initial phase of the program called on the Authority to consult with all 56 States, territories, and the District of Columbia, to ensure that public safety's voice was heard and reflected in the development of the NPSBN. Subsequently, millions of data points, encompassing multiple public safety disciplines, were included in the request for proposal. After an open and competitive process, AT&T was awarded the contract to build, operate, and maintain the network. In 2017, every Governor—from American Samoa to Maine—chose to adopt the FirstNet model for deployment of the NPSBN.

With over 2.8 million Network connections and more than 18,500 agencies utilizing the network, there are first responders trusting FirstNet with their lives, every day in your districts, and across the country, and that is a responsibility that we take very seriously. It has taken years of consultation, developing trust with public safety partners across various, diverse backgrounds, to reach where we are today. Unlike other communications solutions, the FirstNet Authority is in a unique position where we work solely in the interest of all of public safety—including Federal, State, local, and Tribal—and for the communities that strive to keep each and every person in this country safe. As the challenges that the public safety community faces evolve, we at the FirstNet Authority will strive to provide the communication tools required by public safety to protect the American public.

Following the infusion of $7 billion from the Spectrum Act, the FirstNet Authority is a financially self-sustaining program and not reliant on appropriated funding from Congress. Through the FirstNet contract, AT&T makes annual payments for access to the FirstNet Authority's licensed Band 14 spectrum—the license for which must be renewed by the Federal Communications Commission (FCC) next year to allow the FirstNet program to continue—which funds our operating costs and additional investments in the Network for public safety.

Through our forward-looking technology Roadmap[5] and investment program, the organization's focus continues to be consulting with public safety to prioritize Network investments for the greatest impact. Based on public safety's feedback, the FirstNet Authority's first set of Network investments expanded the fleet of deployable assets dedicated to FirstNet users and began upgrading the FirstNet Core for initial 5G capabilities.

---

[2] The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States ("9/11 Commission Report"), available at *https://www.govinfo.gov/app/details/GPO-911REPORT/*.

[3] See 9/11 Commission Report at 397.

[4] See S. Rep No. 112–260, at 3 (2012), available at *https://www.congress.gov/112/crpt/srpt260/CRPT-112srpt260.pdf*.

[5] SeeFirstResponderNetworkAuthorityRoadmap, *https://firstnet.gov/system/tdf/FirstNet__-Roadmap.pdf?file=1&type=node&id=1055*.

Next February, the Government Accountability Office (GAO), as required by the Spectrum Act, will present their recommendations to Congress regarding FirstNet's 15-year sunset provision, which is slated to go into effect in 2027. I look forward to working with this committee, and indeed all of Congress on the details of GAO's recommendations.

LOOKING BACK: LEARNING FROM PUBLIC SAFETY

Looking back at that fateful day, now more than 20 years ago, there are numerous stories of public safety officials lacking the basic communication tools required to support mission success. All of us in the community know the stories of public safety officials writing notes on pieces of paper and running them around Ground Zero because all communications capabilities were down. I'm sure that many of us here today can recall instances where commercial systems were saturated due to high demand. I think back to when I was a Congressional staffer for this very committee back in August 2011 when the earthquake in Virginia caused the House offices to shake and for the buildings to be evacuated. Communicating with our loved ones was almost impossible on that day given that the commercial networks were overwhelmed by the demand.

While many of us on Capitol Hill lived that moment for the first time in 2011, public safety had been experiencing such scenarios since before September 11, 2001. This committee, and indeed the whole of Congress, knew that the time had come that something needed to be done, and FirstNet was that solution.

As such, public safety asked for a network specifically built for their mission, utilizing dedicated Nation-wide spectrumas recommended in the 9/11 Commission's report, and Congress heard that call with the creation of FirstNet.

As the FirstNet Authority planned for the Network, we consulted public safety in all 50 States, 5 U.S. territories, the District of Columbia, and across Indian country, as well as leveraged the expertise and experiences of our Public Safety Advisory Committee (PSAC),[6] to ensure the Network reflected public safety's broadband communications needs. Public safety told us the network needed to be affordable, reliable, interoperable, and custom-built for them. The network solution needed to be designed to work in dense urban areas, where challenges come in the form of urban canyons, in-building coverage dead zones, and subway tunnels; and likewise, the network needed to provide coverage in rural parts of our country, where previously the business case did not exist for the commercial providers to build mobile broadband networks. That input was instrumental in creating the network we have today and will continue to inform the network of tomorrow.

The mission of the PSAC is to assist the FirstNet Authority in carrying out its statutory duties and responsibilities.

A TRULY NATION-WIDE NETWORK

One of the challenges in designing a Nation-wide network for public safety has been finding solutions that meet the many unique needs of first responders across the country. To address that challenge, in 2017, the FirstNet Authority worked with AT&T, our Nation's Governors, the State Points of Contact, and public safety leadership in the States to design individualized FirstNet State plans to build out the Network and meet public safety's needs. These State plans detailed the initial 5-year Network deployment for each State, with expanded coverage and capacity in rural, suburban, and urban areas. While Governors had a choice to "opt-out" and build their own State networks, all Governors across all 56 States and territories ultimately decided to "opt-in" to the FirstNet build.

By March 2018, the FirstNet Authority and AT&T officially began the Nationwide Network deployment and offering public safety services, such as priority and preemption, to FirstNet subscribers. AT&T remains ahead of schedule on the Nation-wide deployment and is anticipated to have almost completed the initial 5-year network buildout (originally slated for 2023) by the time the FirstNet Authority seeks renewal of its FCC license in late 2022. Since the Network is operational and serving thousands of public safety users today, we believe that it is clearly in the public interest to renew the FirstNet Authority's FCC license so that the FirstNet Authority can fulfill its mission throughout the life of the 25-year agreement with AT&T.

---

[6] Under the 2012 Act, the FirstNet Authority was required to "establish a standing public safety advisory committee." 2012 Act § 6205(a)(1) (47 U.S.C.§ 1425(a)(1)), Pub. L. No. 112–96, 126 Stat. 156 (2012). The FirstNet Authority established the PSAC in February 2013 consisting of members representing all disciplines of public safety as well as State, territorial, Tribal, and local governments. The PSAC also has at-large members and Federal members.

Today, we are over 3 years into the deployment of FirstNet's dedicated Band 14 on both new and existing towers, and already we have seen the Network make a major difference in the lives of first responders and the communities they serve.

NETWORK PERFORMANCE DURING JANUARY 6, 2021: WHY DEDICATED SPECTRUM MATTERS

Earlier this year, the FirstNet network was stress-tested by an event where priority and preemption and a dedicated network proved critical to local first responders right here in the District. As Dr. Chris Rodriguez—Director of Washington, DC's Homeland Security and Emergency Management Agency—testified before this subcommittee last month, Washington's local first responders utilized the FirstNet service and dedicated FirstNet deployable units in response to the January 6, 2021, attack on the U.S. Capitol building.[7]

During the response, multiple public safety agencies used FirstNet service so that first responders could communicate. Where commercial network calls failed and texts and videos could not be sent or received due to congestion caused by a surge in traffic, FirstNet worked. As reported by *PC Magazine:*

"As mobs stormed the U.S. Capitol, plenty of people nearby reported their phones having no signal or non-functional connections . . . The cops' phones all keep working because they're on a special part of the AT&T network called FirstNet, which gives priority to first responders."[8]

SUPPORTING PUBLIC SAFETY DURING THE PANDEMIC

Upon the deployment of FirstNet and the availability of its services, public safety has relied on the network to serve its broadband communications needs. Notably, we have seen an increase in the use of FirstNet during the pandemic—a sign that the network is helping public safety carry out its mission in the face of COVID–19. Health care workers and responders are using FirstNet services at COVID–19 testing centers, field hospitals, and vaccination distribution sites across the country. We are seeing an increase in the use of data to confront the pandemic at nearly double the rate of consumer data traffic.

First responders are taking advantage of FirstNet for telehealth as well as adapting the use of the network in creative ways to fit the needs of their specific operations. For example, hotspots and smartphones powered by FirstNet are enabling 9–1–1 telecommunicators to take calls and dispatch operations from their homes and remote locations. This enables agencies to allow for social distancing among their staff, keeping these front-line essential workers safe so they can continue to serve the community.

Throughout the pandemic, the city of Alexandria, Virginia's, emergency communications center (ECC) has relied on FirstNet to support remote operations. Using hotspots and smartphones powered by FirstNet, Alexandria dispatchers are able to take calls from their homes and remain in contact with staff on-site. The FirstNet Push-to-Talk (PTT) solution, enabling FirstNet phones to act as two-way radios, ensures that telecommunicators working from home are as connected and ready to respond as if they were still back at the call center. Palm Beach County, Florida, 9–1–1 call centers also have depended on FirstNet to enable remote dispatching and call-taking. Similarly, the Oglala Sioux Tribe's Department of Public Safety relies on FirstNet to keep their police officers connected to ECC dispatch when they are responding to an incident. FirstNet supports applications that enable dispatchers to transmit mission-critical information to responders and remain in touch with them as they respond to an incident.

In addition to supporting remote call-taking and mobile communications, FirstNet can act as a secondary network for ECCs in case of a primary network failure. These applications will only grow in their importance as ECCs transition to Next Generation 9–1–1, in which data needs to be able to travel in and out of an ECC in a quick and seamless manner.

FirstNet also has improved interoperability on the Network through supporting mutual-aid efforts, including situations where ambulances are called in to assist from outside a hard-hit region. Paramedics using FirstNet devices and enhanced PTT capabilities can seamlessly communicate and work together with neighboring agencies. As we do for all major emergency operations, the FirstNet Authority will continue to gather public safety use cases and best practices from the response to

[7] See: *https://homeland.house.gov/imo/media/doc/2021-10-7-EPRR-HRG-Testimony-Rodriguez.pdf.*

[8] See: *https://www.pcmag.com/opinions/why-cell-networks-cut-out-at-the-us-capitol-riot.*

COVID–19 so that agencies and practitioners can learn from each other and further understand how the Network can support their communications needs.

In the midst of a pandemic, responders must address and prepare for other emergencies. FirstNet has been there to assist with its dedicated fleet of deployable assets to augment coverage and capacity, including during the tornadoes in the southeastern United States, wildfires across California and the West, and during hurricane season along the East Coast and in the Gulf. Prior to major storms, AT&T's FirstNet Response Operations Group (ROG), a team of former first responders who manage FirstNet's response in these types of disasters, staged deployable units and back-up generators outside the path of the storm. Immediately following storm systems, the ROG team coordinated with State emergency operations centers, local agencies, and Federal Emergency Management Agency Urban Search and Rescue teams to deploy Satellite Cell on Light Trucks (SatCOLTs), and generators to impacted areas to support public safety communications efforts on the ground.

FIRSTNET INVESTMENT AND INNOVATION

The FirstNet Authority will continue to deliver for public safety and drive innovation. Since the signing of the 25-year contract with AT&T in March 2017, we have made substantial progress in build-out, innovation, and investments back into the Network for public safety.

Here are recent innovations and investments to support our Nation's first responders:

- *Z-Axis*.—One of the key capabilities that public safety requested during the planning phase of FirstNet was the ability to determine the vertical location of personnel within a building, also known as Z-axis. Knowing what floor of a building a firefighter is on is critical information to have during an emergency. This technological challenge that public safety identified for FirstNet, and that we worked with AT&T on to deliver a solution, is now a reality. The FirstNet Authority is proud to say that this service is now available and being rolled out on the Network in markets across the country.
- *FirstNet PTT*.—The FirstNet Authority has been working with global standards bodies for years to ensure public safety achieves a PTT solution that supports mission-critical services capabilities. FirstNet was the first to market with a Nation-wide, mission-critical, standards-based PTT solution. Earlier this year, the network began launching solutions for LTE interoperability with Land-Mobile Radio (LMR) systems. FirstNet now gives public safety agencies using traditional two-way radios access to communicate seamlessly with smartphone users on FirstNet PTT. These gateways act as a technological bridge between LMR technology and 4G LTE smart phones.
- *5G Investments for Public Safety*.—The FirstNet Authority recently took the first step to begin evolving the FirstNet Core to prepare for 5G technology—ensuring that FirstNet continues to evolve with industry technology enhancements. AT&T has been upgrading FirstNet's Core infrastructure to enable the higher speeds and greater capabilities of 5G technology for FirstNet subscribers so that first responders have access to the latest in technology innovations. This initial investment to support 5G technology is already in the hands of first responders today, with deployments across the country occurring as I speak. All of this is in concert with our statutory responsibility to consider new and evolving technologies—preparing us for a future where the internet of things and full 5G will help improve public safety operations.
- *FirstNet Deployable Program*.—The FirstNet Authority recently also took steps to expand the fleet of dedicated FirstNet deployables to enhance network coverage and capacity for public safety during emergencies and events.[9] As of June 2021, the FirstNet fleet has 100+ deployables located at sites around the country and U.S. territories that can be sent to emergencies in a matter of hours. The FirstNet-dedicated fleet includes:
  - More than 90 ground-based SatCOLTs and Compact RapidDeployables (CRDs)—SatCOLTs are vehicles with mobile cell sites that connect via satellite and do not rely on commercial power supply, while CRDs are smaller trailer hitch-mounted portable cell sites that can be brought into an area to provide emergency or enhanced coverage.

[9] See FirstNet Authority, *FirstNet Authority Board Approves Network Investments for 5G, On-Demand Coverage* (rel. June 2020), *https://firstnet.gov/newsroom/press-releases/firstnet-authority-board-approves-network-investments-5g-demand_coverage#:~:text=The%20Board%20approved%20%24218%20million%20for%20the%20FirstNet,safety%20turned%20to%20the%20FirstNet%20deployables%20for%20additional.*

- Three Command and Communications Vehicles for emergency deployments, planned events, and training exercises with a space for two communications personnel with multiple monitors, televisions, and charging stations, as well as a large exterior screen and speakers for briefings. These vehicles provide connectivity via LTE (Band 14) and/or Wi-Fi and are able to leverage a variety of backhaul options to connect to the NPSBN. These are also equipped with a generator that can run for multiple days before refueling and includes a lavatory, microwave, mini refrigerator, and sleeping bunk.
- Three airborne Flying Cell on Wings—tethered drones with larger propellers, increased payload capacity, and specialized LTE radios and power systems. Flying Cell on Wings can withstand light rain and wind speeds up to 25 miles per hour and reach heights of up to 400 feet, making them ideal for wildfires, mountain rescues, and other missions where terrain previously made it difficult to maintain connectivity.
- One aerostat—a 55-foot blimp that gives wide-scale portable connectivity over an extended period of time. The aerostat can stay in air for up to 2 weeks and reach heights up to 1,000 feet, making it ideal for large disaster areas like a hurricane's aftermath when sustained connectivity over a broad geographic area is required for response and recovery.

- *High-Powered User Equipment (HPUE).*—FCC rules allow for higher-powered devices to access FirstNet on our dedicated Band 14 spectrum. To leverage this, AT&T recently launched a solution called MegaRange technology.[10] Providing first responders with HPUE can extend the range of coverage where Band 14 spectrum has been deployed significantly. This can be particularly beneficial for public safety users in rural or maritime areas to extend the capabilities of the network.

The FirstNet Authority's Roadmap drives all of these efforts, by ensuring that the voice of public safety is heard and sets a path forward for advancing the capabilities of their network to meet the evolving needs of first responders. The Authority looks forward to continuing to brief the committee on our most recent network advancements and our future plans.

CONCLUSION

In Chairwoman Demings' opening statement in the subcommittee's October 7, 2021, hearing with emergency managers and first responders on this very topic, she—along with other Members—cited the many challenges that still face the emergency communications space. In particular, she noted her first-hand experience as a law enforcement practitioner in the field, serving as Orlando Police Department's Captain of the division stationed at the Orlando International Airport during 9/11. The FirstNet Authority will continue to work with you, Madam Chair, and other leaders in Congress to identify challenges in emergency communications that persist and address them head-on.

The FirstNet Authority will continue to work with public safety stakeholders, AT&T, and our Federal, State, local, and Tribal government partners to build the best network for public safety, and we are proud of the progress we have made to date. Feedback from our public safety stakeholders, on successes and areas for improvement, is critical to our program. Indeed, FirstNet's robust consultation and feedback from public safety has helped us get to where we are today.

We are proud to serve America's first responders in all 50 States, 5 territories, and the District of Columbia. It is amazing to see public safety in rural, suburban, and urban communities across the country—including Tribal lands—integrating FirstNet into their daily and emergency operations. FirstNet's dedicated connection is making a difference and helping them keep safe and protect the citizens they serve. I ask that this subcommittee continue to support the FirstNet Authority—particularly with our spectrum license renewal and reauthorization approaching—as we enter the next phase of this program, to innovate and invest in public safety's network. The support of Congress is critical to FirstNet's and, in turn, public safety's success. This is not the FirstNet Authority's network; it is public safety's network. The public safety community fought long and hard for the creation of the NPSBN, and it is up to us to continue to strive to achieve their vision.

Thank you, and I look forward to your questions.

Mrs. DEMINGS. Thank you so much, Mr. Parkinson, for your testimony. I thank all of our witnesses. I will remind the sub-

[10] See: *https://about.att.com/newsroom/2021/fn__megarange.html.*

committee that we will each have 5 minutes to question the panel. I will now recognize myself for questions.

This question is actually for all of our witnesses, but Director Brown, I just want to repeat something that you said that I really think sets the stage for this hearing. You said when it comes to sharing of information, every second counts. Certainly, as a former first responder, I clearly understand the importance of that statement and the importance of information to men and women, those boots on the ground. Last month, as we have already talked about, we had first responders and emergency managers here to talk about some of the challenges that we face every day. I think no one better understands those challenges than those first responders, emergency managers at the local level. So, Director Brown, I will start with you, how are you supporting and incorporating feedback from emergency managers and first responders on a local level? The question is for all witnesses, but Director Brown, we will start with you.

Mr. BROWN. Thank you for the question. As you are aware, the ability to ensure that we are able to seamlessly move and develop our communications to support responders, it does not happen on the spot during the heat of battle. You know, it really starts early and it is in those forums where we are bringing communicators together to develop effective planning that we are able to receive that kind of feedback and sharing of best practices.

Just this past week, I was in Austin, Texas working with local communicators from the Southwest Border States, Arizona, California, Texas, New Mexico, not only State officials, but also local emergency management officials discussing the effective use of communications planning and the importance of best practices are shared amongst the communicators to ensure that we have the most efficient way of designing communication structures to support incident management.

Mrs. DEMINGS. Thank you so much for that. Mr. Parkinson.

Mr. PARKINSON. Thanks for the question, ma'am. One of the things that we have done at the First Responder Network Authority is develop a number of tools for outreach into the community. So, we have a dedicated team, our public safety engagement group, and what they do is they are positioned throughout the country from really Maine to Hawaii. They were broken up regionally so that these folks are drawn from the public safety community and can engage directly with them. They are drawn from various disciplines, law enforcement, fire, EMS, 9–1–1, emergency managers. We have that dedicated resource because we need that unvarnished voice of public safety to provide direct input into the Authority so that we know what and why we need to make strategic investments into things such as expanding our deployable fleet and 5G and engagements.

Another tool we have is in our FirstNet.gov website. There is a tool there where folks are able to provide, again, direct feedback to the authority. We have a 24/7 open line. We have these opportunities throughout COVID, we were able to do webinars around the country. You have heard me mention the over 1,200 engagements with public safety. That is what we were able to do without being in person. We have a new stakeholder engagement division which

is designed to hold larger groups. Again, once we are in a post-COVID environment, we are really enthusiastic about the kind of feedback that those kind of forums will be able to hold.

We have been able to evolve this. You know, our program was basically founded on consultation with the States back in 2014–2015. We have learned from those consultations. We have learned how to really tweak them, change them, and evolve them. So, we feel very comfortable about the level of engagement we have with public safety knowing that without it, our program would not be able to survive.

Mrs. DEMINGS. Thank you very much. Mr. Johnson.

Mr. JOHNSON. Thank you, Chairwoman Demings. As with Mr. Parkinson there, we also stood up a stakeholder engagement branch within the IPAWS program office to conduct continuous outreach with our State and local governments, first responders, and others. In fact, we have a tremendous engagement with the National Emergency Management Association, as well as with the International Association of Emergency Managers. We just recently returned from the IAM conference with there was tremendous engagement with first responders there, as well as the International Association of Chiefs of Police. So, we try and cover the broad spectrum of first responders to include fire, police, and others who serve our communities. In addition to that, we maintain monthly webinars where we can engage with first responders and emergency managers to gather their feedback on what is working and what is not. Certainly, with that information, we can make the necessary adjustments to serve the broader needs of the community.

Mrs. DEMINGS. Thank you all so very much. The Chair now recognizes the Ranking Member of the subcommittee, the gentlewoman from the State of Florida, Mrs. Cammack, for 5 minutes.

Mrs. CAMMACK. Well, thank you Congresswoman Demings, Chairwoman Demings. My first question is going to be for Mr. Johnson. In 2019, IPAWS added a new Blue Alert event code to allow alert originators to issue an alert whenever a law enforcement officer is injured, killed, missing in connection to any official duties, and/or there are any imminent or credible threat of death or serious injury to law enforcement officers. So, this is a two-parter. Do all of the States, have they—do they have Blue Alert plans in place and they are able to issue these Blue Alerts? To your knowledge, has the utilization of a Blue Alert led to a successful apprehension of a suspect?

Mr. JOHNSON. Ranking Member Cammack, great question. We worked with the Department of Justice, the Community Policing Office, to establish the Blue Alerts that are being sent in response to a police officer either being injured or who is missing in the line of duty. We are aware that there is a pretty aggressive outreach campaign within the Department of Justice to assist States with developing their Blue Alert plans. I have seen that Blue Alerts have been issued, for example, in the State of Texas, where a suspect actually injured a law enforcement officer and a State-wide Blue Alert was issued. That suspect was apprehended within a matter of hours, not days. Once that Blue Alert was issued to the public and then public, you know, public engagement in the process

assisted law enforcement with identifying the suspect and reporting on his whereabouts.

We have seen that take place in a number of States across the country where Blue Alerts are being used very effectively. I believe down in Florida there may have been one or two. I can get back to you on that where the Blue Alert—where Blue Alerts have been issued in response to law enforcement activity and the perpetrator still being on the loose.

Mrs. CAMMACK. It might have cut out a little bit in the beginning. I wasn't sure if I heard you. Do every State—do all the States have a Blue Alert in place or are we still doing the outreach trying to get every State on-board?

Mr. JOHNSON. So, the Department of Justice's COPS office or Community Policing Office is responsible for working with State police and others to establish their Blue Alert plans. At last report, I think over 40 States had Blue Alert plans that were being exercised. But I would have to go back and check with the COPS office to see exactly where that stands today.

Mrs. CAMMACK. Thank you, Mr. Johnson. If you could follow up with my team in writing of what the current status is and how we can help expedite that to make sure that every State has this Blue Alert in place, that would be really helpful.

The next question for you, Mr. Johnson, is one of the recommendations from the National Advisory Council on Modernizing the Nation's Public Alert and Warning Systems was to encourage the use of public media broadcast capabilities to expand alerts and warnings and interoperable communication capabilities to fill the gaps in rural and underserved areas. Specifically, what has FEMA done and what steps has FEMA taken to address this recommendation?

Mr. JOHNSON. Ranking Member Cammack, thank you so much for the question. I seem to have drawn a blank. But with regards to public broadcasting and the ability to reach people regardless of where they are, what they might be doing, or who they are, has been one of the primary goals of the IPAWS program office in FEMA to ensure that No. 1, we can create this type of ubiquitous alerting environment where we can leverage all of the Nation's technology to reach people to inform them of threats to their safety. We have been engaged with public broadcasters, as you are aware. Public broadcasters and broadcast capabilities tend to be extremely resilient and survivable during disasters. In fact, during Hurricane Irma and Leah in Puerto Rico and St. Thomas, we saw that our broadcasters remained on air while most of the other communications methods were, you know, extremely devastated and remained in an outage-type state for several weeks.

We continue to work with public broadcasters to ensure that we cannot—that we leverage their services in member stations, as well as the rest of the broadcast community. In fact, we are connected into over 20,000 broadcasters across the country who leverage our services to communicate any, you know, public safety information or warnings to the general public. The same applies to the wireless industry and 65 wireless carriers we are connected into for wireless emergency alerts. And NOAA's Weather Radio, we are leveraging those capabilities. There are 1,000 transmitters across the country

to also provide additional reach. So, we are using just about every platform that is possible in the country to serve as dissemination channels to reach people where they are.

Mrs. CAMMACK. OK. Thank you. Thank you, Mr. Johnson. Mr. Brown, I actually have a couple questions for you. I know my time——

Mrs. DEMINGS. The gentlewoman's time has expired. Maybe we will have time for a second round. The Chair now recognizes the gentlewoman from Texas, Ms. Jackson Lee, for 5 minutes. If you can turn your camera on? Ms. Jackson Lee. We will move on to the gentleman from New Jersey, Mr. Payne, for 5 minutes.

Mr. PAYNE. Thank you, Madam Chair. Thank you for this timely hearing. My question is for Mr. Johnson and Director Brown. My bill, H.R. 615, the DHS Interoperable Communications Act, which is now law, requires that the Department submit to this committee a strategy for achieving and maintaining interoperable communications among DHS components. To both you gentlemen, how are you taking what came out of these reports and then incorporating it into your work?

Mr. JOHNSON. Thank you, Congressman Payne. On the FEMA side, we made some, I think, fairly aggressive steps to provide for interoperability of the Nation's alert and warning capabilities. In fact, back in 2010, we adopted the common alert protocol that was developed by the organization for structured information systems. Within that particular standard, we identified the IPAWS USA profile that would define what an alert and warning would consist of. So, on the front end, where State and local governments are using alerting authorities to push information throughout IPAWS out to multiple dissemination channels, that standard allows for interoperability or the ability of disparate types of alerting tools to partner and leverage IPAWS services.

The same applies on the back end with disseminating information to the public. The public now, or the broadcast industry, the wireless industry, as well as our other technology providers, can subscribe to that one standard and ensure that one message is disseminated over multiple platforms. It also provides an opportunity for innovation by our technology providers with their knowing that there is a common standard that can be adopted or utilized to develop their technologies from further reach of alert and warning to the community.

Mr. PAYNE. Thank you.

Mr. BROWN. Thank you for the question. As Director Johnson mentioned, FEMA and CISA are in partnership along with other components in the Department to ensure that we are working together collaboratively to ensure that communications interoperability is improved. One of those initiatives includes the effective development of a training curriculum for communications unit leaders and communications technicians to ensure that effective planning occurs between components within the Department to achieve interoperable communications. That is one of the initiatives that we are undertaking. Additional initiatives include the participation in a forum that we call One DHS and a forum that we call the Joint Wireless Program office to discuss the challenges of interoperable planning and use of tactical communications amongst the

components within the Department. That in effect, is also a representative of setting the example across the Federal space with the other departments and agencies that the wisdom of the bill that you sponsored and was enacted, you know, allows for the Department to create an example of how one Federal agency can create interoperability amongst its varied parts. The Emergency Communications Preparedness Center, which the 21st Century Emergency Communication Act of 2006 established, is a forum that we share the progress made by that One DHS as an example to the other departments to emulate.

Mr. PAYNE. Thank you. Mr. Johnson, also, in January 2018, Hawaii's Emergency Management Agency sent out an erroneous incoming ballistic missile alert as we have discussed here. What lessons has the agency learned from this incident and how are you supporting and incorporating feedback from States?

Mr. JOHNSON. Thank you for the question, Congressman Payne. The unfortunate incident that took place on January 13 at approximately 8:07 in the morning was really unfortunate and created a great deal of panic for the people of Hawaii. We have learned a number of lessons from that unfortunate event and have taken several steps to ensure that that does not happen again. As an example, we have revamped our training that is offered through the Emergency Management Institute for both operators of our alert and warning systems, as well as emergency management leadership. We have established monthly proficiency demonstrations requiring all alerting authorities to demonstrate proficiency in the use of their internal systems with IPAWS. And to do that in a safe environment leveraging our technical support services facility that provides 24/7 support to our alerting authority should they have any issue with drafting an alert, questions on whether the system should be used for in response to a particular event, or with any other challenges that they may have.

We have worked with private-sector application developers to improve the tools that they are using by alerting authorities. In fact, we have sent several letters to them recommending improvements to their products. However, one of the challenges that we have with these companies is that FEMA does not actually have a contractual relationship with these companies. So, our recommendations are just recommendations to these companies. But I can tell you that when we issue these letters with recommendations from FEMA, most of the software vendors who are providing these tools to State and local governments tend to pay attention and they are aggressively adopting those recommendations.

But in addition to that, we conduct weekly or monthly webinars. We provide tips on use of the system should there be any question on, you know, emerging themes that we are seeing from across the community. We will take one additional step by issuing tips on the use of the system or whatever the issue may be to the broader community to ensure that they are aware of those things.

Mr. PAYNE. Thank you.

Mr. JOHNSON. Then our working groups provide for continuous engagement and feedback from the community as well.

Mr. PAYNE. Thank you very much, Madam Chair, I will yield the balance of my time. Thank you.

Mrs. DEMINGS. The gentleman's time has expired. The Chair now recognizes the gentleman from Louisiana, Mr. Higgins, for 5 minutes.

Mr. HIGGINS. Thank you, Chairwoman and Ranking Member and thank you for holding today's hearing. I very much appreciate our witnesses for being here today. Effective emergency communications are critical to States that are subject to impact by a natural disaster like hurricanes response and recovery. It just cannot happen without effective communications that have been stabilized and policies and procedures that are in place to position our first responders to use that technology that we are talking about today. In 2020, after back-to-back hurricanes, southwest Louisiana faced many challenges with communications. So, the technology we are discussing today that is used to restore internet and cell connections can certainly be an asset to communities that are vulnerable, as well as an important tool for first responders that are tasked with actually responding and helping a community to recover. So, Mr. Parkinson, interestingly, it is my understanding there was a FirstNet public safety blimp operating in my district in Cameron, Louisiana following the hurricanes in 2020. Can you please describe to the committee what the purpose of the blimp was and how it aids and in recovery and first responders' ability to do the job and help impacted communities. Talk to us about the blimp.

Mr. PARKINSON. Yes, sir. So, I have got an image here just of the blimp there you have it. That is the FirstNet One blimp.

Mr. HIGGINS. Right, that is it.

Mr. PARKINSON. That is the one, yep. That was flown outside in Cameron Parrish, Louisiana following the disaster of Hurricane Laura, sir. What it is designed to do is to be tethered and go up to about 1,000 feet and, in essence, it acts as a floating cell phone tower. It is able to radiate coverage over many tens and tens of miles. So, in a situation where Cameron Parrish, which as you know, was completely devastated by Hurricane Laura, from infrastructure to, you know, communications capabilities, to utilities, we were in a position with FirstNet to take the FirstNet One blimp and launch it for the first time and provide communications capabilities. You know, this FirstNet One blimp is but one of over 100 assets that we have in our deployable fleet. These include CRDs, these are compact rapid deployables. You can throw these on the back of a pickup truck. We also have more deployables that are slightly larger formed factors in the shape of trucks. So, what we try to do at first is build into the program a state of resiliency that allows for different form factors that provide different solution sets so that as we see different scenarios play out from the ground for public safety, we have a communications and recovery capability that can meet the needs of public safety in the FirstNet——

Mr. HIGGINS. How is that—how is it integrated with local law enforcement? How do first responders interact with the technology, a new technology you are describing?

Mr. PARKINSON. Yes, sir. So, any first responder network authority subscriber can call out these assets at zero additional cost. So, if you are paying $45 a month to recall out for one of these blimps or for one the deployables, it does not add another penny to one's—to an agency bill or anything like that. That is unique to FirstNet.

So, sir, as you are using your FirstNet device, you have access to these type of solutions sets. So, in the event of hurricane recovery, disaster wildfire recovery out west, just as another example, this provides additional coverage in areas where the network maybe temporarily down, for example.

Mr. HIGGINS. That is fascinating. Madam Chair, it is incredibly important this information that we are bringing to the table today. I thank you again and the Ranking Member. I am sure my time has expired and I yield.

Mrs. DEMINGS. Thank you so much, Mr. Higgins. You had another minute but thank you for yielding. The Chair now recognizes the gentleman from Texas, Mr. Green, for 5 minutes.

Mr. GREEN. Thank you, Madam Chair. To my friend, Mr. Higgins, I will gladly accept that time that you did not use, sir. Good to see you dear brother Higgins. Always enjoy your comments. Thank you, Madam Chair. Madam Chair, I am very fortunate. I have been blessed to represent a district wherein the ballot is printed in English, Spanish, Vietnamese, and Chinese. We live in a polyglot society across the length and breadth of this country. Linguistics are exceedingly important when we have these natural disasters. I am concerned about how people who don't speak English, they are not proficient with English, how do they receive proper communications with reference to resources and other concerns that they may have? So, I will direct to my question to Mr. Johnson, Director Johnson, and Director Brown. Can you share with me some intelligence on how persons who are not English proficient but we know they are here and we know that they will need help as well. How do the receive the communications necessary to be better informed when a disaster strikes?

Mr. JOHNSON. Thank you, Congressman Green. A very good question in terms of communication and, you know, the acknowledgment of the broad demographics within our communities and people who don't have an understanding of the English language. Certainly, we here at FEMA are charged with ensuring that all Americans who reside here have access to alerts and warnings to include those with access and functional needs as well as those without an understanding of the English language. We have done several things to ensure the broad dissemination of alerts and warnings. One, as I mentioned, we adopted the common alerting protocol and within that determined the IPAWS USA profile within the standard. That allows for multiple information blocks with the opportunity to enter multiple languages into a single message.

The challenge that we have on the front end is that many of our alerting officials at the State and local level don't possess the language capability to craft those messages in the languages that are spoken in those communities. Currently, today we support English and Spanish as you mentioned. But there a multitude, as you mentioned, of other languages that are spoken in these communities.

The other half of the equation is to downstream dissemination technologies that are used that don't necessarily support languages outside of English and Spanish currently. Now, we are working with the State of Minnesota who has an initiative entitled, ECHO Minnesota where they are actually through broadcast radio transmitting languages in English, Spanish, Hmong, Somali, and

Hmong and there is a broader initiative to put those type services through APIs and the web to allow others within the emergency management community to draw upon those services and those type technologies.

But first we have to have the skill sets on the front end to craft the messages and then the downstream dissemination technologies have to be able to support those things as well. So, like we have here at FEMA allow for multiple languages within our house.

Mr. GREEN. Well, thank you very much. Let me just share an additional thought with you and I will be as terse as possible. I was in Mexico. I was on a bus and the driver stood up and said something in Spanish. I speak very little Spanish. After the driver said this, everybody rushed off the bus. They ran over to a line and they stood in line. So, later on as I am trying to get and I am the last person, I said what is going on? The driver explained to me that this bus was out of service because it needed repairs and that the next bus would not hold as many passengers as the bus I was on. So, last in line, I don't make the bus that is going to get me where I need to go. It is really a challenge when you don't understand the language and something important is going on. So, my follow-up question to you is, what kind of time line do we have? Have we established a time line to perfect not only the technology, but the personnel necessary to do this? In my district, we speak over 80 different languages. Can you help me, please?

Mr. JOHNSON. So, thank you, sir. Within FEMA, it is a continuous engagement to broaden our capabilities to ensure that everyone in this country has equal access to alert warning information, certainly where there is some threat to their safety. We have made those accommodations in IPAWS to allow for multiple languages. In fact, we have not been able to test in an environment where we have exceeded the capability of IPAWS through the common alerting protocol to support up to, you know, 100 to 200 languages. The challenge that we have is on the front end with just States and locals having those language capabilities within their organizations. Then second with the technology if we were to develop a technology that would provide for language, on-the-fly language translation, there is a huge distrust of technology to make those on-the-fly translations on the part of the emergency management and public safety community.

But I can tell you that we are going to continue to aggressively pursue that. We will work with NEMA and IAM and others to protype these technologies and to develop trust and confidence in these technologies when they are called upon. We will continue to keep that at the forefront of our agenda in terms of equal access to information that is being made available——

Mr. GREEN. Thank you.

Mr. JOHNSON [continuing]. Regarding threats to public safety.

Mr. GREEN. Thank you, much. Madam Chair, for edification purposes, can you share with me how much time I have left?

Mrs. DEMINGS. The gentleman's time has expired. If we have time, we will do a second round of questions.

Mr. GREEN. Thank you, Madam Chair. I greatly appreciate your indulgence. Thank you.

Mrs. DEMINGS. The Chair now recognizes the gentlewoman from Iowa, Mrs. Miller-Meeks, for 5 minutes. Mrs. Miller-Meeks, I believe you are still muted.

Mrs. MILLER-MEEKS. I need to unmute. It just didn't recognize my finger touch. So, thank you so much and thank you for, Madam Chair, for having this important hearing. You know, Iowa is no stranger to natural disasters especially those that knock out communications. In August 2020, a powerful derecho swept across the midwestern United States and it caused severe damage and serious damage in Iowa. In response to requests from public safety, the FirstNet response operations group deployed portable generators and portable cell sites to boost FirstNet connectivity where coverage was disrupted due to infrastructure damage and loss of commercial power. Since the derecho, AT&T has made significant investments in permanent power at lower sites in Iowa. In addition to deploying new permanent infrastructure, the dedicated fleet of FirstNet portable network assets are available 24/7 at the request of FirstNet subscribed agencies and at no cost to public safety. The FirstNet deployable assets make sure first responders have connectivity when and where they need it both during and after planned large events and during times of emergency. The fleet of 100-plus dedicated deployable assets includes ground-based assets such as satellite cells on light trucks. The FirstNet satellite cells on light trucks provide similar capabilities and connectivity as a cell tower. The portable assets link to the FirstNet via the satellite and don't rely on commercial power availability.

The FirstNet deployable fleet also contains ground-breaking use of aerial cell sites. Flying COWS, Cells on Wings, and FirstNet One and industry first blimp, I think you had showed us, Mr. Parkinson. There are several examples. We have used this during the 2021 RAGBRAI. For those that don't know, that is the Registers' Annual Great Bike Ride Across Iowa. It goes across the entire State with 8 overnight stops. It has also been deployed by the University of Iowa and the university public safety for large events such as the University of Iowa Hawkeye games when typical service may be disrupted or congested.

So, although I have no financial interest in any of the entities that I mentioned, Mr. Parkinson, last month this subcommittee heard from Christopher Rodriguez, the director of D.C.'s Homeland Security and Emergency Management Agency on rapidly deployable cellular infrastructure requested through FirstNet to support the demands of large events and incidents. What different types of deployable assets are currently being used by FirstNet and why are they such an important resource in emergency management?

Mr. PARKINSON. Thank you for the question, ma'am. If I could get a shoutout to the RAGBRAI race. My sister has done it 3 times and, you know, it is a great ride. She has tried to bring me in and so far I have resisted. She is the athlete in the family.

You know, one of the most important things we have had especially as we saw around what Director Rodriguez mentioned a few weeks ago before this very testimony, was the fact that at areas such as the National Capitol Mall, we do need more permanent capacity around the Capitol and down really the Pennsylvania Ave-

nue canyon. You know, there are so many events that take place if you think of the 4th of July annual celebrations. We often see very, very large protests down in those areas. Obviously, the Capitol riots on January 6 is another example. So, there is a need absolutely for more permanent capacity in and around those areas. So, that is one area that we at the FirstNet Authority has been coordinating with many of our Federal agencies who have offices down that portion of the Washington, DC area. I would certainly welcome the opportunity to get more support from Congress in those efforts. So, another important part of it.

Your question though related to deployables, you mentioned most of them. We also have a small fleet of Cell on Wings. These are drones that can fly and create some sort of a mesh network around a certain geographic area. We are always exploring in the space of innovation, trying to identify new capabilities for public safety.

Mrs. MILLER-MEEKS. Yes, I think what is fascinating about it is that with the assets you have be they permanent or they deployable, they function in rural areas or in urban areas. So, it really expands our connectivity, which is especially valuable in emergency situations. I think that answers part of the questions that Representative Higgins had which is our coordination and our first responder group coordinates both with local, so, local law enforcement, local emergency management. So, local, county, State, and then National level. So, there is a coordination in Iowa among all those groups and they are all brought to the table both at the local level and the State level and then with our Federal partners. So, hopefully that will answer some of Representative Higgins question. It has worked very well and has been invaluable in the State of Iowa, especially as I said, during the derecho, which took down a lot of our infrastructure. So, thank you very much for that and, Madam Chair, I will yield back my time.

Mrs. DEMINGS. The gentlewoman yields back. The Chair now recognizes the gentlewoman from New Jersey, Mrs. Watson Coleman, for 5 minutes.

Mrs. WATSON COLEMAN. Thank you very much, Madam Chairwoman and thank you to our witnesses for this very important information. I have a general question for all 3, but I have a very specific question for Mr. Parkinson and then I need to get out of the way.

I understand that FirstNet was the only wireless network that worked reliably for first responders during the January 6 riots thanks to the FirstNet dedicated Band 14 spectrum, as well as a portable telecom infrastructure deployable units brought in for the inauguration. In evaluating how we further strengthen our preparedness for emergency events on the National Mall and Capitol Complex, as we are all aware of the various threats that come our way, do you feel there is a need for more permanent infrastructure on the National Mall and what are the challenges to deploying both permanent and temporary infrastructure on the Mall and around the U.S. Capitol?

Mr. PARKINSON. One hundred percent, ma'am, this is something that we absolutely need. It is something that is without it, there is a constant threat that public safety would not able to have the communications capabilities that they need. So, I certainly would

expand on my previous answer in terms of we need that type of dedicated coverage. We need that kind of dedicated capacity and physical need. So, it is working with the respective agencies that have office space, as well as Federal agencies and the teams who look after the National Mall to get that. So, 100 percent.

Mrs. WATSON COLEMAN. Are there any infrastructure needs in addition? If so, are there any impediments to having it available?

Mr. PARKINSON. Yes, ma'am. So, more fiber is always a good thing, especially as we are gravitating toward 5G ecosystem. So, as we need greater capacity, as we need better technologies, additional fiber certainly would be a welcome asset to be deployed in and around the Mall and the Capitol. How we can work that, how it can be coordinated, we are certainly ready to have those conversations. We started having those coordination conversations with other Federal agencies in around the D.C. area. So, we are happy to provide additional updates to you as those go so that if there are any areas that you may be able to assist with, I would certainly welcome that.

Mrs. WATSON COLEMAN. Greatly appreciate that. For all of the witnesses, really quickly, I am trying to understand all the agencies that are involved in this issue. I am trying to understand all the requirements of people with regard to cybersecurity. I am really sensitive to these issues of redundancies. So, what I would like to know from each of you is the answer to two questions. No. 1 is who are your primary stakeholders? No. 2, if you are only internal, how does your information get externalized? Just for context, we in New Jersey, we were having a tornado warning, which is kind-of unusual, and I am talking to my granddaughter on Facebook and she lives 3½ miles away. She says, hold up mom-mom, we have got a tornado watch going on. She was getting constant updates in her TV. My TV was right in front of me. My phone was right next to me and I got none, 3½ miles away and I can't quite understand what happened. So, if you all could just kind-of tell me your stakeholders and how this all works so that there are people aren't tripping over one another.

Mr. PARKINSON. I will just go very quickly on my——

Mrs. WATSON COLEMAN. I am not being left out.

Mr. PARKINSON. Yes, ma'am. So, on the FirstNet side, by statute, we can only really focus on public safety. That is, we can't offer commercial services. That is up to our partner. We focus on really dedicated men and women in public safety space. We have a very robust engagement program to not only push information out but to receive information.

Mrs. WATSON COLEMAN. OK. So, that is really talking to the first responders on various levels. All right. Mr. Brown and Mr. Johnson.

Mr. BROWN. Sure, just to thank you for the question. To consider the number of Federal organizations that are in the space for cybersecurity, you know, I do like to think about it as a term of concentric and supporting authorities. So, certainly as we work with the FBI, we work with Department of Energy, we work with Department of Health and Human Services and others, that we coordinate the collaboration. Certainly as the National Defense Authorization Act of last year required the establishment of a joint

cyber defense collective, you know, the intent is to work seamlessly together using the authorities that each organization has to ensure that cybersecurity and the availability of supporting our stakeholders, which are all the public safety, which are all of the emergency and management community and as I indicated in my opening statement, the National Security and Emergency Preparedness community.

Mrs. WATSON COLEMAN. Thank you, Mr. Brown. Mr. Johnson.

Mr. JOHNSON. Thank you, Congresswoman. Since the issue of cyber has already been adequately addressed, let me just speak specifically to that tornado warning that was received in your area. The National Weather Service utilizes IPAWS services to push severe weather warnings through IPAWS to your mobile devices and over the emergency alert systems to include their own infrastructure through NOAA Weather Radio. We have made improvements in the system to allow for very targeted areas to be defined that those warnings are relevant for. It could be the case that while your granddaughter received the message or the warning on her TV and on her mobile device, that you may have been outside of the alerted area that was defined by the National Weather Service. The Weather Service looks at all of the criteria that is associated with that event and then has to make a determination on what areas are most threatened by the event and then they will provide immediate notification to those areas. As conditions change, of course, the National Weather Service will provide updates and if your area was, you know, imminently threatened by that event, then, of course, they would have updated that information and in all likelihood you would have received the same information.

Mrs. WATSON COLEMAN. That would have interrupted anything I was watching on TV, right? That notice.

Mr. JOHNSON. It should have, yes. You should have gotten the severe weather warning.

Mrs. WATSON COLEMAN. Thank you, Madam Chair, can you tell me how much time I have left?

Mrs. DEMINGS. The gentlewoman's time has expired. We may have time for additional questions. At this time, the Chair recognizes the gentleman from New York, Mr. Garbarino, for 5 minutes.

Mr. GARBARINO. Thank you, Chairwoman, and thank you to the Ranking Member for having this hearing. As the Ranking Member of the Cybersecurity Subcommittee, I know that cyber risks are some of the greatest threats to our Nation's communications infrastructure. This threat is magnified even more when it comes to the impact it can have on first responders and American lives. Mr. Parkinson, how are FirstNet and AT&T working to ensure cybersecurity protections are baked into the public safety broadband network?

Mr. PARKINSON. Congressman, one of the things we knew when we were developing the request for proposals back in 2015, was that cybersecurity was something that we would have to bake into the program from the ground level up. When you think about cybersecurity in the 21st Century, FirstNet's really the country's only network that thought about cybersecurity from its infancy. A lot of the other commercial networks that are out there had to integrate cybersecurity into their systems. We built it from step one. So, if

you look into our RFP, Section J10, solely focuses on cybersecurity. It provides the requirements that we requested that our proposals looked at when considering cybersecurity. We have a 24/7 knock-and-sock. This is our program that looks just at cybersecurity. This is manned 24/7, 365 by our contractor AT&T. It is something that we take extremely seriously from Day 1.

We also integrate very, very closely from a contractual oversight inspector where there are many, many requirements that our team looks at from cyber risk perspectives. So, we understand the capabilities and the threat to the ecosystem and provide those type of solutions to prevent those from occurring. So, when you look then at the end-user, we are going to have to really be very cognizant of this in a 5G ecosystem as the network gets pushed to the edge and such as device security becomes another important part of that. I know that our partner is looking at that and trying to come up with additional solution sets.

So, again, from our inception to where we are thinking about in the future, cybersecurity is the forefront of everything we do at FirstNet.

Mr. GARBARINO. OK. How does FirstNet interface with CISA to meet, you know, you are working with AT&T and your are contract partners, how do you work with CISA?

Mr. PARKINSON. Yes, I would say this even if Mr. Brown wasn't here today, but we are fortunate enough to have Billy Bob, Mr. Brown, as the DHS representative on the FirstNet board. So, he and I have actually known each other since I was a staffer on Capitol Hill. We have got a terrific working relationship with his team. This is something that even his predecessors had and we look forward to such a very, very close working relationship with the CISA team going forward. So, as I say, from the board level through, we have a very, very strong working relationship not only with CISA, but with many, many other Federal partners.

Mr. GARBARINO. Great. Mr. Brown, I was actually going to ask you next. Do you think—how do you see the relationship between CISA and FirstNet? Do you think they are, you know, things are going well? Or do you think there is room for expanded coordination, you know, to make sure that everything works smoothly and our first responders are protected?

Mr. BROWN. Thank you for the question. But as my right honorable friend, Mr. Parkinson, said that, you know, we have a very close and collaborative relationship between the FirstNet Authority, the FirstNet's contracted partner, AT&T, that built FirstNet, and CISA to ensure that we have a collaborative view on cybersecurity across all of the network service providers.

Mr. GARBARINO. Great. I appreciate the answers, gentleman, and, Madam Chair, I yield back.

Mrs. DEMINGS. Mr. Garbarino yields back. The Chair now recognizes the gentlewoman from Texas, Ms. Jackson Lee, for 5 minutes.

Ms. JACKSON LEE. Thank you, Madam Chair, for allowing us to have this very important hearing and to the Ranking Member as well. I am reminded of the 9/11 terrorist attacks because I was in this building on that day and, in essence, we fled for our lives. We are quite sensitive to the fact that the tragedy of 9/11 evidenced the failures and frailties of that time frame. Having commemorated

the 20th commemoration of 9/11 in New York, it was a stark reminder of the numbers of first responders that we lost that day. An enormous toll on firefighters, who were part of the inability to communicate. I think we will never, never cease to remember certainly that day, but that stain that caused such an enormous loss of life. I think we can say that we have made strides, but I do believe that there is more we can do. These hearings are particularly helpful to us.

Madam Chair, I indicated to you that and hoped that we would discuss H.R. 3060, which is the FEMA Modernization Act that I believe can be very much a part of the work that we are doing in this important committee, creating an Office of Disaster Response, an Office of Disaster Recovery ombudsman, establishment of a National Disaster Medical Triage, and at some point asking the FEMA director to give a report on the level of technology even in the situation where FEMA is engaged in various disaster responses.

I do think that FEMA itself when they are on the ground, leadership is on the ground, needs to have the ability to communicate with first responders because everyone is in a recovery mode. So, I want to raise a question to Mr. Johnson, then a question to our representative from FEMA. Mr. Johnson, in your testimony, you stated that in 2020, twice the number of agencies used IPAWS to send alerts as in 2019, resulting in an 182 percent increase in the number of alerts to the public by local alerting and authorities. Do you think that was effective and as I ask you that question, let me just put into the system number of kind-of alert programs we have. IPAWS, Integrated Public Alert and Warning System, First Responder, FirstNet, and then Emergency Communications Division, and CISA. And the question—and SAFECOM. Are all of these acronyms, are they all working? But in any event, do you have any basis of that?

I want to follow up with a question to Mr. Brown and Mr. Parkinson on the idea of coordinating with these different agencies. Mr. Johnson.

Mr. JOHNSON. Thank you, Congresswoman Jackson. Yes, as stated in my testimony, we did see twice the number of State and local alerting authorities who utilized IPAWS services to amplify information that was coming from the COVID task force as well as the CDC and their local governments with regards to protective actions that could be taken by the general public in response to COVID–19. We saw State and local governments who were issuing other type of protective action information related to the pandemic. As well as identifying where vaccination locations could be found or with other information associated with curfews and things like that.

Interestingly enough, we saw some extremely interesting use of the system by a number of States who were using the system to issue a wireless emergency alert to mobile devices with a clickable link in there that would take them—take the person to a website that would allow the State to screen for activities that, you know, a person entering into the State——

Ms. JACKSON LEE. If my time runs may I just—sorry, if my time runs out, would you welcome a protocol of technically and tech-

nologies capabilities with dealing with all of the subsets of these communication systems in times of disaster? Would that be helpful?

Mr. JOHNSON. Absolutely, yes, ma'am.

Ms. JACKSON LEE. So, enhanced communication and technology would be helpful to you. Let me quickly—thank you so very much. Let me quickly go to Ed Parkinson. You said more was needed to be installed to improve communications for wireless technology. What is the basis of that need for improvement? Is it realistic to run more fiber or are there other technology fixes? Mr. Parkinson.

Mr. PARKINSON. I would say that is a start, ma'am. What you see when we have events like the 4th of July celebrations, there are these super COWS on wheels, the massive vehicles that are prepositioned prior to these events taking place. As more and more people leverage more and more technologies, as we migrate toward 5G, the pressure on networks both FirstNet and commercial is going to ever grow. So, we will need additional capacity in and around the Mall and the Capitol. So, yes, ma'am, something we certainly need.

Ms. JACKSON LEE. Thank you. Mr. Brown.

Mr. BROWN. Thank you.

Mrs. DEMINGS. The gentlewoman's time has expired. Hopefully, we will——

Ms. JACKSON LEE. Thank you, Madam Chair.

Mrs. DEMINGS [continuing]. Have time for an additional round. I believe that completes all of the Members in the first round. If there are other Members who wish to participate in a second round, I ask that you please turn your cameras on at this time. Ms. Jackson Lee, I am assuming that you are going to participate in the second round. OK, all right. All right.

Ms. JACKSON LEE. I muted, yes. Thank you.

Mrs. DEMINGS. OK. Thank you. Then we will begin the second round of questioning. I will recognize myself. This question is directed to Director Brown. You know, one of the biggest emergency communications concerns is the outdated 9–1–1 infrastructure. Of course, we know to enhance the 9–1–1 system, our Nation is moving forward with the roll-out of Next Generation 9–1–1 with capabilities that rely heavily on the internet to accept and process a range of information including texts, images, video, and voice calls. We talked about some of the cybersecurity concerns with FirstNet, but Director Brown, what are the cybersecurity concerns with uploading the Next Generation 9–1–1 system onto one mainframe and what is the ECD's plan to prepare for any, God forbid, cyber attacks?

Mr. BROWN. Thank you for the question. As we consider broadly across the Nation, the public safety answering points, there are roughly 6,000 State and local public safety answering points across the Nation, but that is not the complete picture. There are another, that we know of, 1,500 public safety answering points, although they are called by a different name that exist on Federal reservations. Whether those are part of the Parks Service, part of the Department of Defense's military installations, part of the labs, installations that the Department of Energy has, the Federal footprint also has these call centers or whatever they may be called that op-

erate current 9–1–1 services that will need to migrate to Next Gen 9–1–1 as well in order continue to provide services to citizens that may in harm's way or in danger on that installation property.

One of the challenges that we have been discussing and working with our 9–1–1 partners across the Nation is the idea that we understand that the provision of text, videos, or images to the call centers provides the possibility of the introduction of malware. The last time we met with the committee, we explained as we have worked with partners across the Nation, the criticality of the emergency communications ecosystem that includes a notification from citizens of challenges, includes Government-to-Government responder coordination, includes alerts and warnings notification from Government to citizen, and also includes that citizen-to-citizen communication and transfer of information, which includes nonprofit organizations or disaster recovery organizations and critical infrastructure as well as sharing insights to provide for disaster response. If malware is introduced from the beginning in an image, in a video, in a text, to a 9–1–1 center, it has the possibility and potential of providing that malware to those interconnected Government systems.

Here at CISA, we have been discussing this issue sharing and beginning a process of sharing the concerns of cybersecurity public safety answering points across the Nation. We certainly in the past year, have had several discussions with more than 15 States about the challenges presented by cybersecurity including ransomware as we prepare for the Next Gen 9–1–1 introduction.

Mrs. DEMINGS. Mr. Brown, thank you so very much for that very thorough answer. How can we as Members of Congress assist in your efforts to make sure that we are able to protect the public but also make sure that we protect our systems as well?

Mr. BROWN. Thank you for that follow-up. The continued leadership that the committee is providing, the continued support for the initiatives that the CISA is making to try and address the challenges in 9–1–1 are a part of the equation as all of the components across the Government. We know that FCC has some play. NTIA has some play. Department of Transportation's National 9–1–1 Program Office has some play. All of us working together as supported by the committee are how we will ensure that first responders and citizens across the Nation are able to take advantage of the Next Gen 9–1–1 capabilities.

Mrs. DEMINGS. Thank you so much, Mr. Brown. I want to check to see if the Ranking Member Mrs. Cammack, is with us? OK. I see Mrs. Watson Coleman from New Jersey, are you? OK. I will call on the gentlewoman from Texas, Ms. Jackson Lee, for her follow-up questions.

Ms. JACKSON LEE. Thank you very much, Madam Chair. Again, I am really interested in, among other things, is a reform of FEMA during its work on disasters giving a more pointed focus on handling disaster circumstances that befalls many of us. In fact, now, disasters are not relegated to hurricanes, Chairwoman. They are tornadoes. They are fires. They are flooding in places where one had not seen it before such as the terrible flooding that occurred in the East Coast just a few months ago.

So, let me go back to that question. Let me frame one question dealing with a question of my colleague on January 6. I didn't see any accelerating utilization of technology. It looked as if there was difficulty in our first responders Capitol police, being able to reach out and to communicate. What do you feel is the Achilles heel when you have circumstances of danger like that when you cannot communicate? Would you want to take that question, Mr. Brown?

Mr. BROWN. Thank you. The challenge as you articulated, is that the more time that it takes to understand the incident, determine what resources are needed, and then effectively marshal those resources, you know, that is what, you know, as I mentioned in the opening statement, that, you know, every second counts. You know, that really is, as we recognize, you know, it could be the difference between life and death and certainly as a destruction of property is involved being able to have communications for emergency response officials to provide that assistance to the public once they are notified of that is critical. Having redundant systems, having, you know, a constellation of partners that are working together to ensure that First Responder National Security and Emergency Preparedness personnel are able to seamlessly receive that information interoperably is the critical component of the equation.

Ms. JACKSON LEE. In the course of your work with CISA, it looks like you did a survey, I understand, in just a while ago in your statement, you acknowledge that you did a survey and approximately half of the public safety communications, I mean, organizations reported their LMR systems are more than 10 years old. Seventy-six percent of public safety organizations have no or insufficient funding for capital investments. How does that impact, for example, a crisis of terrorism and/or a crisis of a disaster, which we see happens across the Nation, this antiquated equipment? Mr. Brown.

Mr. BROWN. Thank you for the question and noting the SAFECOM Nation-wide survey. As you well know, one of the challenges that we face in continuing to understand the evolving difficulties facing first responders across the Nation is our ability to actually ask questions, you know, the Paperwork Reduction Act presents challenges sometimes. You know, as we are preparing to do our next SAFECOM Nation-wide survey, you know, we have had to start now because it will take us 2 years to try to get through the process to ask a simple, ask some simple questions to understand, you know, the evolution of challenges and requirements. But as we look at, you know, how the responders are able to actually provide, you know, support on the ground, you know, it is really that forward planning, that development of relationships, and establishment of collaborative cooperation amongst responders from many different jurisdictions, many different agencies, many different disciplines that——

Ms. JACKSON LEE. That need updated technology, which is it looks like the gist of your report. Is that correct?

Mr. BROWN. Yes, ma'am.

Ms. JACKSON LEE. They need updated technology. So, that is something that we should focus on in the Federal Government in collaborating with our local partners.

Mr. BROWN. And as we have seen across the Nation at the local level recognizing their fiscal challenges.

Ms. JACKSON LEE. Mr. Parkinson, you mentioned, as a follow-up to my earlier question, 5G communications is being sold as a solution to faster better communications. Is this the case? Why is 5G communications causing communications challenges for first responders? I guess, I would add, Mr. Parkinson, does everybody have it?

Mr. PARKINSON. No, ma'am. So, in the commercial network right now that are out there, 5G we are still in its infancy. If you think about every generational upgrade, it takes about 10 years. So, we are only about 2 years tops to the phase now within 5G. I wouldn't say it is a challenge right now. What I would say is because we are at the infancy of 5G, the community, the public safety community, as well as the commercial world is still trying to figure out what exactly 5G capability is going to hear and bring. We are very aware of what we see in marketing and so on, but in terms of the public safety community, how is public safety going to integrate 5G? I think of things at the enterprise level. So, as a law enforcement officer returns to her station, she is able then to hopefully in a 5G ecosystem, in a smart police station in the future, automatically download all of the images, data, and so on, that she has been able to capture out in the field before she gets back to her workstation. When you think of the lower latency and the ability to say have livestream 5K video—4K video—I beg your pardon—from a camera on that individual and that officer streamed back to the incident commander. There are all type of capabilities that we can envisage in a 5G ecosystem. But until we get to where 5G is holistically adopted, not only in the public safety space, but at the commercial space, the real benefits of 5G will not be realized. I still think we are some time away from that. It is coming. It is coming fast, but we are not quite there yet.

Ms. JACKSON LEE. The Federal Government have a role to play?

Mrs. DEMINGS. The gentlewoman's time has expired.

Ms. JACKSON LEE. Thank you, Madam Chair.

Mrs. DEMINGS. Thank you so much. The Chair now recognizes the gentleman from Texas, Mr. Green, for 5 minutes.

Mr. GREEN. Thank you very much, Madam Chair, especially for this second round because it is extremely important. I am going to lay a proper predicate for my question. Outside of my Congressional office window, I can see an overpass. Under that overpass, there are people. This is their home. This is where they wake up in the morning. This is where they go to work. They solicit from the public passing by. Here is my concern. When there is a natural emergency or natural disaster, in law we call these things, Acts of God, when these things occur, how do we make sure that these people get the necessary information to protect themselves to make sure that they can get the resources that they need? What is FEMA doing to help us with this? Again, Director Johnson, I will go to you. I don't mean to appear to be picking on you, but you seem to be a good source of information. Can you share some intelligence with us, please?

Mr. JOHNSON. Thank you, Congressman Green. One of the things that, you know, if you look at FEMA's ready.gov website, there is

a lot of information on the site regarding, you know, the types of actions that every person in this country can take to be better prepared for some of the threats or disasters that they may encounter in their communities.

Mr. GREEN. If I politely intercede for a second.

Mr. JOHNSON. Yes, sir.

Mr. GREEN. My suspicion is, and, listen, I am not trying to be cute if I say this. But my suspicion is that they are probably not going to access that website given their status and their station in life.

Mr. JOHNSON. Right, thank you, sir. So, one of the, I think, the beauties with our alert and warning capabilities is the opportunity to receive disaster or alert and warning information over a broadcast radio. Broadcast radio has proven to be extremely resilient over the years. It is extremely affordable in that it is free. And has served as a vital communications lifeline during disasters. That is one of the basic or fundamental investments that we are making in partnership with broadcasters across the country is to ensure that that broadcast capability remains viable for the future and that it remain free for the consumer of that information.

A lot of folks think that, you know, as you mentioned, these folks are not going to have potentially access to the internet or other services and information that we post on websites, not even some of the social media tools that we utilize at the State and local level to communicate information. Which is why we invest in broadcasters that common denominator across the Nation that provides extremely broad coverage and that is free to every consumer within the country. That is one way——

Mr. GREEN. May I politely——

Mr. JOHNSON [continuing]. Through those common platforms. Yes, sir.

Mr. GREEN. If I may I would like to politely intercede again. What about this as a possibility? A layperson who knows little of what he speaks, but what about simply having a truck sound equipment? We know where they are, literally. That Houston, I could map it out for you where people are. There are some places where communities have developed. Could we not simply use that sort of sound equipment to let them know that perhaps they can go to this National Broadcasting System that you are talking about or maybe they should check other sources, but something as simple as that probably could alert them so that they can then apply additional intelligence. What are your thoughts?

Mr. JOHNSON. Right. So, I think—thank you very much, sir, for the question. I think if you look across the country in many communities, for example, where there are nuclear power plants, there are emergency planning zones that have been established where the use of sirens become very important, you know, should there be some type of mishap at a nuclear facility. I have seen or observed that across the country in many communities are utilizing sirens to get that initial broadcasting information out to local populations. But I think it is going to require a concerted effort on the part of State and local governments, our cities and municipalities, along with the Federal Government to solve some of those challenges.

Mr. GREEN. I thank you. I would like to be a part of the solution. So, if there is any way that we can work together, I really do care about the folk outside my window living under the bridge. If I can work with you, I would appreciate it. Thank you again, Madam Chair. A excellent hearing. Greatly appreciate your calling this to our attention. Thank you.

Mrs. DEMINGS. Thank you so much. The gentleman yields back. With that, I want to thank the witnesses for their valuable testimony and the Members for their questions. The Chair reminds Members that the committee record shall be kept open for 10 days. Without objection, the subcommittee stands adjourned.

[Whereupon, at 11:36 a.m., the subcommittee was adjourned.]

# APPENDIX

QUESTIONS FROM CHAIRWOMAN VAL DEMINGS FOR ANTWANE JOHNSON

*Question 1.* FEMA has invested in Primary Entry Point (PEP) stations, which consist of mostly AM stations, that connect to the National Public Warning System. Cars are typically built with radios that have helped millions receive alerts when internet services are down. Have you seen a trend of newer cars or designs eliminating car tuners? If yes, how is IPAWS working to ensure that there are no emergency communications gaps created by the elimination of car tuners?

Answer. The Federal Emergency Management Agency (FEMA) Integrated Public Alert & Warning System (IPAWS) is 100 percent dependent on private-sector technologies and participation for delivery of alerts and warnings to people. We are aware of automobile manufacturers trending toward eliminating AM tuners in new model electric car offerings and providing AM tuners as an option in other automobiles. If this trend indicates that AM radio will no longer serve as a viable and sustainable long-term method for providing emergency alerts and information to the population in the future, FEMA will seek industry, U.S. Department of Homeland Security (DHS) Science and Technology Directorate (S&T), and the Federal Communications Commission (FCC) input on sustainable private-sector communications infrastructure to meet our requirement for a National alerting system capable of delivering emergency alerts and information across the spectrum of National hazard scenarios.

*Question 2.* In 2017, a spokeswoman for Sonoma County, California, stated "officials chose not to send out a WEA because it would target too large a geographic area, evacuating residents who weren't in danger and causing gridlock on the roads."[1] What is being done to ensure geographic accuracy for emergency alerts, and how does IPAWS collect feedback after an alert is sent?

Answer. FEMA IPAWS does not have technical capability to collect information about where an alert was delivered after it is sent. The IPAWS office continues to work with private-sector alerting participants and the FCC to improve the geographic relevance of emergency alerts. In April 2018, the FCC adopted rules to improve the accuracy with which Participating Commercial Mobile Service (CMS) Providers transmit Alert Messages to the specified target area. The rules require CMS Providers to deliver a message to 100 percent of the Wireless Emergency Alert (WEA) enabled devices within a specified geographic area, with no more than 1/10th of a mile (or 528 feet) overreach. The IPAWS office participated in the Alliance for Telecommunications Industry Solutions standards group to develop changes to the wireless interface specifications to support the 2018 FCC rule changes. In December 2019, FEMA fielded IPAWS Open Platform for Emergency Networks (IPAWS OPEN) WEA 3.0 functionality supporting enhanced geotargeting capabilities. IPAWS OPEN WEA 3.0 includes delivery of location data for an alert to WEA 3.0 capable phones with location services enabled to determine whether the device should display and alert based on their location relative to the targeted alert area specified by an alerting authority. The wireless industry began deploying WEA 3.0 for enhanced geotargeting in early 2020. The Cellular Telecommunications Industry Association (CTIA) Wireless Association (industry organization that represents many of the CMSPs) estimates that 34 percent of consumer phones support enhanced geotargeting in 2021 and that the majority of phones in circulation by the end of 2022 will support the enhanced WEA 3.0 geotargeting capability.

*Question 3.* An increasing amount of people are streaming content on their televisions instead of using cable or watching local broadcasting networks. How are you working with streaming platforms to ensure that their users can receive emergency alerts?

[1] Andone, Dakin, "Californians Say They Didn't Receive Emergency Wildfire Alerts," CNN. October 2017. *https://www.cnn.com/2017/10/13/us/california-fires-emergency-alerts/index.html*.

Answer. FEMA IPAWS stands ready to deliver messages to streaming media platforms and any other distribution platform that conforms to the Common Alerting Protocol (CAP). CAP is an international standard developed by the Organization for the Advancement of Structured Information Systems and was adopted by FEMA in 2009. IPAWS is designed to provide alert information in a standard CAP form that is easily transported and consumed by internet-based applications. Additionally, FEMA participates in the on-going FCC proceeding and Notice of Inquiry (PS Docket Nos. 15–91 and 15–94) to explore the feasibility of including streaming services in the Emergency Alert System regulations. The IPAWS office has engaged with various streaming providers and is diligently seeking a streaming provider willing to voluntarily monitor and consume alerts from the IPAWS feeds and present alerts to their customers.

*Question 4.* In 2018, in Paradise, California, some neighborhoods were never told to evacuate as a fire swept in and devastated a community, and according to several reports, local leadership did not use the Wireless Emergency Alert (WEA) system. What are you doing to ensure that communities are aware of IPAWS?

What type of trainings are local emergency managers receiving to know when it is an appropriate time to send out an IPAWS alert?

Answer. Agencies using the IPAWS are required to complete IPAWS Independent Study course IS–247, IPAWS for Alert Originators. Additionally, the IPAWS office continuously engages emergency management and public safety practitioners to increase awareness and understanding of how IPAWS works and provides guidance and tips for how to effectively alert and warn the public. Engagement includes a monthly webinar series, frequent IPAWS Tip and Advisory emails to more than 6,000 recipients, website updates, strategic event attendance at National, State, and private-sector emergency management conferences, social media engagement, and maintains a digital library of alerting guidance.

The IPAWS Technical Support Services Facility (TSSF, formerly known as the IPAWS Lab) is a closed environment that allows State, local, Tribal, and territorial alerting authorities to safely test, train, and exercise IPAWS alert dissemination capabilities. Alerting authorities can practice and see how alerts sent via IPAWS interact and present as Emergency Alert System activations on radio and television, Wireless Emergency Alerts on cellular phones, Non-Weather Emergency Messages on National Oceanic and Atmospheric Administration (NOAA) Weather Radios, and other services and devices that interact with the IPAWS All-Hazards Information Feed.

The IPAWS TSSF enables public safety officials to gain confidence using IPAWS in this practice and training environment without disseminating messages to the public. Additional purposes of the IPAWS TSSF include alert and warning, functional assessments, alert dissemination validation, training, procedural, and process evaluation, and functional requirement validation.

The IPAWS Modernization Act of 2015 (Pub. L. 114–143) tasked FEMA with establishing an IPAWS subcommittee to the National Advisory Committee (NAC) to address "Modernizing the Nation's Public Alert and Warning System. In response to the February 15, 2019 NAC report, recommendation 2 (FEMA should develop simple alert and warning jurisdictional and multijurisdictional plan templates and tools to provide guidance and best practices for emergency alerting.), the FEMA IPAWS Office collaborated with DHS S&T to release the IPAWS Program Planning Toolkit (IPAWS Program Planning Toolkit/FEMA.gov) and began an outreach campaign to encourage its use. The toolkit provides a free, interactive, web-based interface that helps alerting authorities create a comprehensive all-hazards alerting plan inclusive of staff planning, standard operating procedures, tests, and exercises. The toolkit also contains an alert messaging template creator to help authorities prepare custom alert message drafts for anticipated threats in their area.

*Question 5.* In February 2020, GAO issued a report (GAO–20–294) stating that some State and local public safety agencies cannot access IPAWS and others have low confidence using it. One of the recommendations made by GAO was for IPAWS to establish procedures "to prioritize pending IPAWS applications and to follow up with applicants to address these applications." According to GAO's website, this recommendation is still open.

When do you think this recommendation will be resolved?

Answer. Changes to internal FEMA processes for approving applications allowed the FEMA IPAWS office to clear the backlog of pending applications in September 2019. We continue to improve application processing and are in the final stages of implementing an automated application processing system that will further streamline the process and provide application status tracking. The automated application processing tool is currently undergoing system accreditation and is expected to be available in the third quarter of fiscal year 2022.

QUESTIONS FROM RANKING MEMBER VAL DEMINGS FOR ANTWANE JOHNSON

*Question 1.* On August 21 of this year, FEMA conducted a Nation-wide test of the Emergency Alert System (EAS) and Wireless Emergency Alerts (WEA). What were some of FEMA's take-aways from this test?

Answer. The 2021 test of the National Public Warning System and Wireless Emergency Alerts demonstrated the technical means to rapidly disseminate a message via multiple modes of communication in a quick and efficient manner when seconds matter. The August 2021 test was the sixth Nation-wide test of the Emergency Alert System (EAS) (radio and television) and the second test of WEA distribution Nation-wide. The August 2021 WEA test was the first test in which the new opt-in WEA test category was used to send a National message that would only be received by phones where wireless customers opted in to receive "test" messages.

FEMA used the National Public Warning System Primary Entry Point (PEP) radio stations to initiate the 2021 EAS test by broadcasting a National Periodic Test message. Radio and television providers "listen" to a PEP station or to another station that is listening to a PEP station in accordance with FCC-approved State EAS plans. All radio and television providers that are part of the Emergency Alert System are required to demonstrate monitoring and rebroadcast of a National test message in accordance with FCC rules.

Final analysis and results of the 2021 test are pending. Based on preliminary reporting, we anticipate a 5 percent improvement over 2019 EAS test results.

Result summary of previous IPAWS Nation-wide alert tests:

- 2011—EAS via PEP
  - 84.6 percent of reporting EAS stations received and broadcast the test message
- 2016—EAS via IPAWS–OPEN
  - 94.9 percent of reporting EAS stations received test message
  - 86.8 percent of reporting EAS stations broadcast test message
- 2017—EAS via IPAWS–OPEN
  - 95.8 percent of reporting EAS stations received test message
  - 92.1 percent of reporting EAS stations broadcast test message
- 2018—EAS and WEA via IPAWS–OPEN
  - 95.9 percent of reporting EAS stations received test message
  - 90.9 percent of reporting EAS stations broadcast test message
  - ~75 percent* of people in the United States, received the WEA "Presidential" test message
- 2019—EAS via PEP
  - 84.3 percent of reporting EAS stations received test message
  - 81.5 percent of reporting EAS stations broadcast test message
- 2020—did not test due to National COVID response activities.

*Question 2.* FEMA recently established a 24/7 IPAWS Help Desk, to provide real-time assistance to alerting authorities who are experiencing issues with IPAWS. What type of usage has the 24/7 Help Desk had so far? Has FEMA received any feedback from alerting authorities about the Help Desk?

Answer. The IPAWS Modernization Act of 2015 (Pub. L. 114–143) tasked FEMA with establishing an IPAWS subcommittee to the NAC to address "Modernizing the Nation's Public Alert and Warning System." In response to the February 15, 2019 NAC report, recommendation 2 (FEMA should develop simple alert and warning jurisdictional and multijurisdictional plan templates and tools to provide guidance and best practices for emergency alerting) and recommendation 5 (Establish 24/7 FEMA IPAWS Help Desk to support AOs in the use of the system), FEMA launched the 24/7/365 TSSF in March 2021. The IPAWS TSSF has supported on average 30–50 Alerting Authority engagements per month. These engagements vary in complexity but typically include technical assistance to successfully issue live alerts, monthly proficiency demonstrations, drill and exercise guidance, IPAWS overview and instruction webinars, and response to general questions regarding alert and warning practices and procedures. Feedback from Alerting Authorities regarding the support provided by the 24/7/365 technical support services facility has been outstanding. Besides numerous accolades and acknowledgements, the IPAWS technical support services team is regularly requested to provide IPAWS subject-matter expertise to FEMA regional training initiatives, FEMA National Integration Center Technical Assistance webinars, FEMA National Exercise Division, and other industry-related events highly attended by public safety alerting authorities. These efforts increase awareness of the IPAWS Technical Support Services Facility and the capabilities readily available. Of particular note has been the IPAWS TSSF technical support

*Based on independent publicly posted survey results.

to the State of Texas and issuing a State-wide Blue alert on behalf of the Texas Department of Emergency Management in response to a Law Enforcement Officer being injured in the line of duty and the assailant being at large. Additionally, the IPAWS TSSF assisted numerous counties in resolving technical issues that led to the successful amplification of COVID–19 Task Force and the Center for Disease Control and Prevention guidance via WEA messages to communities and communicating local jurisdictional protective actions.

QUESTION FROM HONORABLE VAL DEMINGS FOR BILLY BOB BROWN, JR.

*Question.* CISA has not updated the 2015 Communications Sector-Specific Plan, even though DHS guidance recommends such plans to be updated every 4 years. Does the 2015 plan provide adequate guidance to protect the communications sector from new and emerging threats?

Is CISA planning to release an updated plan? If yes, please provide the time line. If no, please explain.

Answer. The Communications Sector's approach to risk management outlined in the 2015 Communications Sector-Specific Plan addresses how public/private partners collaborate to identify and mitigate new and emerging risks. The Cybersecurity and Infrastructure Security Agency (CISA) works extensively with public/private partners to identify new and emerging risks and publish guidance to address those risks, as outlined in the plan. These public/private partnerships include, but are not limited to, the National Security Telecommunications Advisory Committee, the Enduring Security Framework, and the Information and Communications Technology (ICT) Supply Chain Risk Management Task Force.

CISA will update the Communications Sector-Specific Plan upon completion of the refreshed National Plan, which is expected next year. The refreshed National Plan will incorporate key provisions of the Fiscal Year 2021 National Defense Authorization Act that codified and clarified Communications Sector Risk Management Agency (SRMA) roles and responsibilities. It will also be informed by the Communication Sector Coordinating Council's report, "Moving Security Forward (March 2021)," that provides a comprehensive overview of its strategic approach on maintaining reliable and resilient communications in the wake of cyber threats and impacts from the pandemic.

CISA's update of the Communications Sector-Specific Plan will reflect these updates and incorporate concepts and ideas from several products and initiatives completed since the previous Communications Sector-Specific Plan was developed, including a July 2021 Communications SRMA Fact Sheet and a Communications Sector Profile.

In addition, a cornerstone of CISA's efforts to strengthen and enhance emergency communications capabilities Nation-wide is the National Emergency Communications Plan (NECP), developed in partnership with Federal, State, local, territorial, Tribal, and private-sector stakeholders. Subchapter XIII of the Homeland Security Act of 2002, as amended, requires CISA to develop and periodically update the NECP. Updated in 2019, the NECP identifies current gaps to achieve interoperable emergency communications and promotes innovation and integration of new technologies while considering associated risk. In particular, the 2019 NECP update incorporates a new goal related to cybersecurity, noting that as cyber threats and vulnerabilities grow in complexity and sophistication, it is critical that public safety organizations take proactive measures to manage their cybersecurity risks. For additional details on cybersecurity support, please visit the NECP Spotlight on Ensuring Interoperable Encrypted Communications.

QUESTIONS FROM HONORABLE KAT CAMMACK FOR BILLY BOB BROWN, JR.

*Question 1.* As we all are aware, with increased technologies to improve first responder communication systems comes increased cyber vulnerabilities. We heard from our witnesses in our October hearing regarding steps they're taking or have taken to increase their cybersecurity posture. One witness testified that even for a rural county, they have a very robust response to cyber threats; however, their office has had no engagement with CISA. How is CISA engaging with the smaller, more rural first responder community?

Answer. Managing risks associated with advances in technology requires not only having an understanding of new threat vectors such as cybersecurity challenges to internet protocol-based technology, but also knowledge of the interface risks posed with older technologies still used in parts of the Nation. Newer technologies make the Nation's emergency communication more efficient but also expose them to the risks and vulnerabilities inherent in information technology and operational technology. CISA proactively engages with stakeholders across the Nation including

smaller, more rural communities to address current and future threats even as technologies evolve. Small, rural communities receive no-cost technical assistance through CISA, when requested, to support interoperability planning, governance, and training and exercises on a variety of topics including cyber-focused services to rural first responder organizations. Below are a few additional examples of cyber-focused services that CISA provides to rural communities:

- Congress authorized CISA to establish the Rural Emergency Medical Communications Demonstration Project, a $2 million competitive grant program, with awards in 2016, 2018, and 2020. The grants were awarded to the University of Mississippi Medical Center, which proposed to use existing communications infrastructure, improve operational effectiveness, and provide communications training to enable improved rural medical services through its First Hands Program and First Voice Program, as well as other enhancements. In addition to vast notable accomplishments from expansive training to improving first responder access to information while in the field, the effort was recognized for saving at least 8 lives as a result of the training and resources provided. For more information, please visit the NECP Spotlight on Enhancing Rural Emergency Communications Capabilities.
- Through the Interoperable Communications Technical Assistance Program, CISA provides all States and territories with direct support in the form of State-wide planning workshops and technical assistance (TA) training, tools, and resources. Since 2008, more than 2,550 TAs have been delivered to all States and territories. In addition to specific, tailored assistance, CISA provides support to develop and implement State-wide Communication Interoperability Plans that enable States and territories to align and prioritize their communications needs and advocate for funding to their local and State governments.
  - CISA offers customized cyber-focused TA for Public Safety Emergency Communications Centers, 9–1–1 Systems and Land Mobile Radio functions to mitigate ransomware/Telephony Denial of Service attacks on public safety networks, and systems that affect 9–1–1 and emergency communications.
  - The CISA Ransomware Infographic is available to all stakeholders and has been delivered to rural counties in States such as Missouri and Kansas to help educate staff on cyber threats to public safety communications and serve as foundational assessments for cyber planning and resiliency.
  - Communities who would like to learn more about CISA's services, should contact their State-wide Interoperable Coordinator or regional CISA Emergency Communications Coordinator.
- To meet evolving Information and Communications Technology needs, CISA's Communications Unit (COMU) program, which outlines the functions, positions, training, and certifications required to support interoperable incident communications, includes an Information Technology Service Unit Leader position and course to assist incident command in managing the confluence of voice, video, and data communications and information, cybersecurity, and application management for incident planning and response. To date, more than 17,000 personnel have been trained to fill COMU positions.
- Through the Tribal Emergency Communications Program, CISA supports Native American and Alaska Native tribes through consultative engagement, outreach, advocacy, technical assistance, and inter- and intra-agency coordination to ensure strengthened public safety operable and interoperable communications. CISA works individually with Tribal communities to assess and document how their customs, public safety communications capabilities, challenges, infrastructure, and current governance structures impact decision making, management, and resource allocation. Additional information is located here:
  - CISA Tribal Emergency Communications Resources Fact Sheet
  - CISA Tribal Emergency Communications Program Infographic–2021
  - CISA Tribal Emergency Communications Program Brochure
  - NECP Spotlight: Working with Tribes to Achieve Interoperability.
- CISA also maintains a robust regional security advisor cadre that focuses on physical, emergency communications and cybersecurity critical infrastructure. CISA's Regional security advisors conduct outreach, deliver security assessments, and offer technical assistance upon request.