Testimony

Billy Bob Brown, Jr.

Executive Assistant Director
Emergency Communications Division
Cybersecurity and Infrastructure Security Agency

U.S. Department of Homeland Security

FOR A HEARING ON

Emergency Communications

UNITED STATES HOUSE OF REPRESENTATIVES
HOMELAND SECURITY COMMITTEE
SUBCOMMITTEE ON EMERGENCY PREPAREDNESS, RESPONSE, AND COMMUNICATIONS

November 2, 2021

Washington, DC

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.

The State of Emergency Communications

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 Statewide 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 Nationwide Survey (SNS), which is a nationwide 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 nationwide 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 five years, the survey also indicated:

- Approximately half of the public safety organizations reported their LMR systems are more than ten 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.

Statewide and Tribal Planning

Through the Interoperable Communications Technical Assistance Program (ICTAP), CISA provides all states and territories with direct support in the form of statewide 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.

Statewide 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 statewide 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 statewide 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 onsite support to states and jurisdictions and situational awareness to CISA leadership. CISA staff members also provide Emergency Support Function #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 911 system. CISA will provide direct assistance to jurisdictions across the U.S. to implement NG-911 capabilities and ensure cybersecurity interconnectivity and interoperability amongst those systems using common standards nationwide. Among the benefits of nationwide interoperability are the ability to respond to 911 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 911 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, 911 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-911 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.