TESTIMONY OF EDWARD F. DAVIS III, FORMER COMMISSIONER OF THE BOSTON POLICE DEPARTMENT and FOUNDER OF THE EDWARD DAVIS COMPANY

LESSONS LEARNED: AN EXAMINATION OF MAJOR SECURITY INIDENTS AT MASS GATHERING EVENTS

TASK FORCE ON ENHANCING SECURITY FOR SPECIAL EVENTS IN THE UNITED STATES
COMMITTEE ON HOMELAND SECURITY, U.S. HOUSE OF REPRESENTATIVES

July 22, 2025

Chairman McCaul, Ranking Member Pou and distinguished Members of the Taskforce, I would like to thank you for the opportunity to testify at today's hearing and to contribute to this important discussion on how the lessons learned in the 12 years since the Boston Marathon bombings can help drive meaningful security advancements as the United States prepares for a series of major upcoming special events — including the FIFA World Cup and the 2028 Olympic and Paralympic Games. It is critical that we apply those lessons to strengthen our collective preparedness, incorporating advancements in intelligence and technology, enhancing interagency coordination, and ensuring the safety of all who participate.

The tragic events of the 2013 Boston Marathon — a terrorist bombing that claimed the lives of Lu Lingzi, Krystle Campbell, Martin Richard, Officers Sean Collier and Dennis Simmonds, and left hundreds injured, forever changed the City of Boston. While the impact of that day will never be forgotten, the collective response has served as a catalyst for transformation. This incident reshaped how law enforcement, public officials, the media, and the broader community prepare for and respond to major emergencies. It highlighted the critical importance of interagency coordination and real-time communication strategies. The lessons learned continue to inform our approach to safeguarding public events, managing crisis response, and conducting complex investigations into terrorism. As we plan for future major events and incident response, the Boston Marathon bombing stands as a stark reminder of the stakes — and a testament to the importance of preparedness, resilience, and unified action.

The response to the attack demonstrated that effective preparedness depends not only on planning but also on seamless collaboration and the critical importance of intelligence cooperation across all levels of law enforcement agencies and government. Close coordination between local, state, and federal agencies was essential to ensuring public safety. This integrated effort was instrumental in the successful identification and apprehension of the suspects. The Boston Regional Intelligence Fusion Center (BRIC) served as a central hub for intelligence gathering during and after the attack. As one of the intelligence-sharing nodes established by the Department of Homeland Security, the BRIC synthesized information in real time from surveillance footage, social media monitoring, citizen reports, and law enforcement databases. This centralized and collaborative approach significantly accelerated the identification of critical evidence and suspects. The performance of the BRIC underscored the value of integrated intelligence operations and led to broader national investment in fusion center capabilities. This highlighted their role as force multipliers in complex emergencies by breaking down agency silos and enabling a unified response. To best safeguard against evolving threats, intelligence agencies must remain open to collaboration — not only sharing what is known, but actively seeking out what is unknown through cooperative efforts across jurisdictions. Equally important is how that information is communicated, as intelligence is only as effective as the clarity, context, and timeliness with which it is received and understood by those who must act on it. This mindset starts with leadership; the tone set by the chief matters, because what their leaders say, the officers do.

While the fusion center's intelligence response was swift in Boston, the City of Los Angelos used lessons learned from Boston by integrating Emergency Operations Centers into the fusion centers to proactively embed the LA's Emergency Management Department software during the 2022 Super Bowl, enabling minute-by-minute threat analysis for on-the-ground tactical teams. Another tool exemplifying the benefits of interagency coordination is the Department of Homeland Security's Special Event Assessment (SEAR) Rating. SEAR ratings are voluntarily submitted for special events, which are sent to DHS's Office of Operations Coordination by state, local, and federal officials for an overall risk assessment. This intelligence is critical for on-the-ground security planning. The SEAR rating is currently utilized for major events such as the Super Bowl and Kentucky Derby, and I would highly encourage it for the upcoming events as well. As the United States prepares to host upcoming global events such as the FIFA World Cup and the Olympic Games, the continued integration of fusion centers into emergency operations and interagency collaborative resources like the SEAR rating will be critical to facilitating real-time communication, coordinated decision-making, and effective threat mitigation across all levels of law enforcement.

As I have previously testified to this committee, during the Boston Marathon Bombings, cell network capabilities dropped for all of those in the direct vicinity of the attacks. The overwhelming number of phone calls, texts, and internet searches rendered voice communications practically useless for everyone, including the police officers on the scene and those responding. With a lack of a secure network, communications between municipalities, local and federal law enforcement were impeded, and change was critically important. In the years since, technological advancements have played an important role in enhancing investigative capabilities and public safety since the 2013 Boston Marathon bombings.

As a member of the Board of Advisors for AT&T and the company's FirstNet platform, I've seen the public-private partnership of FirstNet take on this challenge and improve first responders' ability to communicate on scene. The goal of FirstNet is to provide law enforcement and first responders with the ability to access a highly secure and completely reliable service network during times when commercial servers become overwhelmed, exactly when it is needed most. In 2018, the network launched "The FirstNet Core, a physically separate and highly secure infrastructure that creates a differentiated experience for first responders. FirstNet ensures an encrypted, end-to-end communication network for law enforcement. This partnership works for first responders.

Another aspect of technology that has seen significant improvement is AI capabilities of video and photo surveillance, both private and public. It has been well documented that the use of video surveillance from Boylston Street restaurants and photos provided by spectators who were at the scene of the attack led to the identification of the two suspects and provided a timeline of their movements after the attacks, leading to their apprehension. While video surveillance can sometimes carry a negative connotation, it is essential to respect the fundamental right to personal privacy. However, in high-profile critical events, a clear cost-benefit analysis demonstrates that the enhanced safety and security provided by identifying and preventing the actions of bad actors outweighs the temporary compromise of privacy in public spaces. Law enforcement combined video with analytic resources available quickly and effectively after the fact. If only we had the tools to prevent it.

At the time of the bombings, law enforcement agencies also faced the challenge of sifting through and verifying information gathered from the scene, tips from the public, and witness accounts, while coordinating interagency decisions on how and when to share verified information with the public. The Boston Marathon Bombing was one of the first incidents where law enforcement utilized the tools of social media, such as "X" formerly known as Twitter, to communicate directly with the public and media agencies. This was the Boston Police Department's most effective way to share pertinent safety information to the masses in real-time. As was published in a white paper I helped pen for the National Institute of Justice's Harvard Executive Sessions on Policing and Public Safety in March 2014, "[The Boston Police Department] successfully used Twitter to keep the public informed about the status of the investigation, to calm nerves and request assistance, to correct mistaken information reported by the press, and to ask for public restraint in the tweeting of information from police scanners. This demonstrated the level of trust and interaction that a department and a community can attain online."[1]

Reliance on open-source data, though, presents real challenges, as the sheer volume of information can both aid and hinder investigations. AI can now create realistic, false images of people and voice replication. As was the case during the marathon bombings, these "deep fakes", when used to interfere or disrupt an investigation, pose a distinct challenge to law enforcement that Congress and legislation must anticipate and prepare for. Deepfakes pose a significant threat to major sporting events by enabling compelling disinformation campaigns that can erode public trust and incite fear. In the lead-up to the 2024 Paris Olympics, a Russian-linked group released a deepfake video of Tom Cruise warning of violence and corruption at the Games, part of a broader effort to undermine confidence in French security and the event itself. These tactics included spoofed news broadcasts, digitally fabricated graffiti threats, and false claims of mass ticket returns. In the U.S., the NFL has also flagged deepfakes and AI-generated phishing as emerging threats, warning that impersonations of players or staff could lead to reputational damage, data breaches, or public panic. As generative AI tools become more accessible, the potential for viral misinformation targeting athletes, teams, and venues continues to grow, making deepfake resilience a crucial component of modern event security.

Deepfakes are just one of the many resources available to cybercriminals. Cyberattacks have emerged as a sophisticated and escalating threat to major sporting events, with high-profile venues and organizations increasingly targeted for espionage, disruption, and extortion. Recent global incidents underscore the scope of this threat: as stated, Russian-linked hackers targeted French Olympic planners ahead of Paris 2024; Iranian actors leaked personal data of Israeli athletes; and ransomware crippled IT systems at the Grand Palais, an Olympic venue. In Asia, China reported over 200,000 cyberattacks against infrastructure supporting the 2025 Asian Winter Games. The threat has grown exponentially—Tokyo 2020 alone saw 4.4 billion cyberattack attempts, prompting agencies like Microsoft and the UK's NCSC to classify sports as high-risk sectors.

In the U.S., the Super Bowl is emblematic of the cybersecurity stakes. This mirrors a broader trend: 70% of sports organizations now experience at least one cyberattack annually, often targeting sensitive financial data, internal communications, or live event feeds. Personal data from athletes and fans is increasingly vulnerable due to the widespread use of digital apps and IoT-connected systems. From data leaks that endanger athlete safety to attacks that disrupt critical venue functions or broadcast feeds, cyber threats now pose a tangible risk to national security, public confidence, and the

[1] Davis, Edward F. , Alejandro A. Alves, and David Alan Sklansky. Social Media and Police Leadership: Lessons from Boston. New Perspectives in Policing (Executive Session on Policing and Public Safety) March 2014.

operational continuity of premier sporting events. A coordinated, layered cybersecurity strategy is no longer optional, it is a prerequisite for safe and resilient event execution.

As technology rapidly evolves, so does the potential for its misuse, with advancements capable of exponentially increasing the risks associated with emerging threats. A striking example is the rise of First-Person View (FPV) drones, which are becoming an increasing concern at major public venues across the United States. Often referred to as the biggest innovation in warfare in decades, FPV drones represent a transformative shift in how aerial threats are deployed, blending low-cost accessibility with high-impact potential. Unlike conventional GPS-stabilized drones, FPV drones are manually piloted, highly maneuverable, and capable of streaming real-time video to operators through goggles or screens. They bypass geofencing restrictions and altitude limitations, enabling them to navigate complex environments, such as stadium entrances, bleachers, or rooftops, with precision and speed. Their analog controls and low radar visibility make them challenging to detect, as they can be launched discreetly from areas like parking lots with little to no advance warning. The unfortunate reality is that it is only a matter of time until this technology is used for terrorist goals. To effectively address the evolving threat landscape posed by the proliferation of privately operated drones, a more robust approach is required, particularly with regard to identifying potential insider threats. This is especially critical in the context of high-profile or special events. For example, in 2014, individuals from Massachusetts were thwarted in an attempt to attack the Pentagon using self-piloted drones; this early attempt underscores the importance of proactive threat assessment and mitigation strategies.

Most recently, during the January 2025 AFC Wildcard game at M&T Stadium, the game was stopped due to the use of an unauthorized drone hovering above the stadium. This incident marked the third drone-related disruption at the venue in two years, highlighting ongoing security concerns about how FPV drones can interrupt and cause potential threats to major events.

Although several promising technologies exist, including jamming systems that can intercept or disable threatening drones, these technologies are expensive and not readily available outside of a military setting. The most glaring concern remains the lack of an acceptable, coordinated response protocol available to state and local law enforcement agencies. A number of bipartisan bills have been introduced over the years; however, these efforts have stalled. The recent executive order helps, but does not go far enough. It is imperative that we prioritize meaningful legislation that equips law enforcement with the necessary tools to address the growing threat posed by the public availability of drones. This absence of a clear tactical and legal framework to respond to drone incursions represents a critical gap in our current public safety strategy, and one that must be urgently addressed to safeguard future events.

As the United States prepares to host a series of high-profile international sporting events, we must draw clear lessons from past domestic incidents like the 2013 Boston Marathon bombings. That tragic event underscored the devastating potential of lone-wolf actors and the vulnerabilities of open-access venues. Since then, the threat landscape has evolved significantly: extremist-driven acts of violence, foreign influence operations, and ideologically motivated terrorism, both domestic and international, have surged across the country. Recent attacks targeting public officials, religious gatherings, and diplomatic personnel reveal a growing pattern of politically and religiously motivated violence, often involving veterans, foreign nationals, or radicalized individuals exploiting ideological divisions. Coupled with rising threats of espionage and terrorism from state and non-state actors such as Iran, North Korea, China, and ISIS, these developments demand a comprehensive security posture. Protecting the integrity of large-scale events now requires not only traditional counterterrorism efforts but also robust intelligence coordination, foreign influence detection, cyber resilience, and proactive community threat assessments.

In closing, while advancements have created a better environment for law enforcement and agencies to respond to crimes, the risk of danger and sacrifice that police throughout our nation face should not be understated. As new technology becomes available to law enforcement, it is also becomes available to criminals and terrorists. New threats, both physical and cyber, emerge daily, especially those related to drone technology and advancements. Police will continue to adapt and overcome but it is critical to ensure a coordinated effort for detection and avoidance is in place. I want to extend my gratitude to our law enforcement and intelligence community partners for their unwavering commitment to protecting our nation. And I thank you and this task force for the opportunity to reflect on the hard-won lessons since the Boston Marathon tragedy 12 years ago—and to consider how we can apply them moving forward. As the United States prepares to take center stage by hosting several major international sporting events in the coming years, we have a unique opportunity to demonstrate leadership, resilience, and innovation in public safety on a global scale.