

*April 8, 2025*

*Testimony of Jon Gruen to the House Subcommittee on Transportation and Maritime Security for a hearing entitled, "America on the Global Stage: Examining Efforts to Secure and Improve the U.S. Travel System and Prepare for Significant International Events."*

Good morning, Chairman Gimenez, Ranking Member McIver, and honorable members of the Transportation and Maritime Security Subcommittee. My name is Jon Gruen, and I am the Chief Executive Officer of Fortem Technologies. I'm grateful for the opportunity to testify today on the timely issue of security in upcoming international events in the United States.

Fortem was founded in 2016 with the explicit intention of developing and producing the technology necessary to defeat a key threat that we saw on the horizon: drones. Nine years later, we have grown to be a global leader in drone detection and kinetic mitigation capabilities, specializing in low-collateral effect systems that can operate safely in populated areas and in the National Airspace. This unique specialty has garnered attention from government agencies and private stakeholders alike, and we are currently deployed at military bases both in the homeland and abroad, with CBP at the southern border, and with dozens of partners across the globe in critical infrastructure and public-event security.

Over the next decade, the United States will host the 2026 Men's World Cup, the 2028 Summer Olympics, the 2031 Women's World Cup, the 2031 Rugby World Cup, and the 2034 Winter Olympics. These are in addition to our regularly held domestic sporting events that frequently surpass 100,000 patrons in attendance.

As we approach these large events in the United States, all of which will have a significant international presence, it is incredibly important to do what this committee is discussing today: analyze what the state of security threats will be to the public and participants at the time of those events, and what should be done now to lower the risk of a security incident.

I started gaining experience in securing large international events as the U.S Special Operations Command lead to the inter-agency Task Force for the 2004 Olympic Games in Athens. At the time, the largest deployment of U.S. inter-agency personnel ever. My recent experiences are based on my company's work providing airspace awareness and counter drone solutions to the 2020 Olympic Games in Tokyo, the 2022 World Cup Games in Qatar, and the recent inauguration of President Trump right here on Capitol Hill.

There are numerous potential threats to large public events, but law enforcement and security personnel have developed capabilities to mitigate most of them. However, there is one threat which evolves every day, and has proliferated at such a fast pace, that law enforcement does not have the tools to mitigate it. Drones are the new weapon of choice for bad actors around the world, posing an escalating threat to security. Public

venues and critical infrastructure, such as airports and energy sites, are equally vulnerable to what might be the greatest asymmetric advantage ever achieved by people intent on death and damage.

As you are well aware, the occurrence of drone threats against critical infrastructure has surged by over 400% in the past five years, with the Department of Defense and Homeland Security reporting thousands of unauthorized drone incidents annually, posing escalating risks to national security. The effectiveness of these drones to cause catastrophic damage is also growing, as displayed in real-time on the battlefields of Ukraine where the development timeline for new drone technologies and tactics is 60 days.

Recent domestic incidents, such as a drone collision with a firefighting aircraft in Los Angeles and a rogue drone that shut down the Steelers-Ravens NFL Playoff game, will happen again at coming attractions if we don't act now. Even larger incidents, such as at Joint Base Langley-Eustis on December 6, 2023, resulted in a near month long inter-agency response to deploy counter drone assets, technology and personnel, all to no avail. Months later a similar incident over a key critical infrastructure site took place in the Pacific Northwest, where law enforcement personnel observed multiple drones flying at consistent intervals for more than a week. In both incidents, traditional drone detect-and-defeat solutions did not work. There was no advanced warning of incoming drones and no countermeasure to defeat what should be considered a clear and present danger.

These incidents have led to the broad acceptance that traditional drone countermeasures are no longer sufficient to protect against what was once thought to be a future threat – Dark Drones, or drones specifically designed to not emit RF signatures and thereby evade traditional drone detection solutions. In order to adequately protect any sensitive site or large public gathering today, dark drone detection and kinetic mitigation must be the core of any successful counter drone system.

Thankfully, we do have the technology to detect, track, and neutralize rogue drones before they cause harm. Companies like mine have developed AI-powered sensors necessary to identify the threats, including Dark Drones, as well as autonomous interceptor drones capable of taking down threats in real-time without collateral damage. Our system intercepts drones with aerial net capture, and then tows them to a pre-determined location, ensuring the safety of bystanders and allowing for forensics on the captured drone. As I mentioned before, this technology has protected spectators at the World Cup, Olympics, the Inauguration and other significant international events. We must field these defensive solutions at scale in the homeland now, as time is a critical aspect in fielding an effective counter-drone system.

Based on our experience, counter drone systems must start to be deployed twelve months before the event. During that time, there needs to be analysis of site-specific layered solutions; hardware must be purchased, delivered, and integrated; teams identified and trained on this new technology; concepts of operations developed; and

small hardware and software modifications made to maximize the effectiveness of those operations.

With the 2026 World Cup just over a year away, we must act quickly to enable relevant federal agencies to procure and deploy these assets as fast as possible and ensure that these agencies and their local law enforcement partners have the authority to act quickly in response to a threat. In a drone attack, seconds count: giving law enforcement personnel on the ground the ability to do their jobs is just common sense.

Currently, the responsibility of countering the threat of drones is spread across multiple agencies with limited authority to counter drone threats in real time. In the instance a drone is detected and determined to be a threat, authorized federal personnel must be present and still request explicit clearance in order to take mitigative action. These barriers prevent even well-prepared organizations, such as owners of stadiums or energy sites, from taking proactive action, and point to a larger systemic challenge that extends beyond large events like the World Cup. The chaos that ensued when unauthorized drone activity disrupted flights at Newark International Airport is a glaring example of our inability to detect and respond in real time.

Long-term resolution to the authorities' challenge has been a topic of debate in Congress for some time, and I am grateful for the thoughtful bipartisan legislation from this Committee's work on H.R. 8610 last year. However, these upcoming events require centralized and streamlined counter-drone processes as soon as possible to ensure their security. In addition, there needs to be delegation of authorities to more state and local law enforcement, even if it is temporary authorization for these events. Their involvement will enable greater flexibility, faster responses, and better security at a 12+ city event like the World Cup where there may not be enough federal personnel or assets to deploy. Empowering state and local law enforcement to defend high-risk locations from unauthorized drones will be critical to success.

We have been lucky that many recent drone incidents were not catastrophic, but luck is not a security strategy. The threat is real, but the solution is within reach. I urge Congress to provide federal agencies with the resources necessary to procure capable counter drone systems as soon as possible, and to make sure that Federal, State, and Local Law Enforcement are granted the appropriate authorities needed to protect these high visibility events. I'm grateful for the opportunity to testify today, and look forward to engaging with all of you on this topic.