**Statement for the Record**

**Mike Sena, President, National Fusion Center Association**

**Hearing: "Before the Whistle: Assessing Information Sharing and Security Collaboration Ahead of Major Events"**

**Committee on Homeland Security**
**United States House of Representatives**

**February 24, 2026**

## Introduction

Chairman Garbarino, Ranking Member Thompson, and Members of the Committee, thank you for the opportunity to testify today on information sharing, intelligence coordination, and security preparations for major national events - where timely, accurate intelligence and effective coordination are essential to public safety.

My name is Mike Sena, and I serve as President of the National Fusion Center Association (NFCA), representing the 80 state and major urban area fusion centers that make up the National Network of Fusion Centers nationwide. I also serve as Executive Director of the Northern California Regional Intelligence Center (NCRIC) and the Northern California High Intensity Drug Trafficking Area (NC HIDTA), where our team works daily with federal, state, local, tribal, territorial, and private-sector partners on threat identification, intelligence analysis, investigative support, information sharing, and operational coordination in collaboration with Real-Time Crime Centers (RTCCs), Fusion Centers, High Intensity Drug Trafficking Areas (HIDTAs), the Regional Information Sharing Systems' (RISS) Watch Centers, and the Center for Internet Security (CIS).

I want to thank Members of this Committee, including Subcommittee on Counterterrorism and Intelligence Chairman Pfluger and Ranking Member Magaziner and Chairman Strong and Ranking Member Kennedy, for including NFCA and our law enforcement association partners in broader discussions on major event security, information sharing, and proposed reforms to DHS intelligence and field operations at the Office of Intelligence and Analysis (I&A). These discussions are critical as we all recommit to securing the homeland from a wide range of threats. Decisions about intelligence reform, field engagement, investigative tools, training, and information sharing systems directly affect how fusion centers and state and local agencies identify threats and respond in real time - especially during major events, where timelines are compressed and consequences are immediate.

Across the National Network of Fusion Centers, more than 3,200 personnel from state, local, federal, and private-sector partners collaborate every day to analyze threats, share intelligence, and support operational coordination, while safeguarding privacy, civil rights, and civil liberties. Since 2001, fusion centers have become a cornerstone of the homeland security enterprise, complementing federal partners such as the FBI's Joint Terrorism Task Forces, the Homeland

Security Task Forces, as well as other DOJ and DHS components. During major national events in particular - such as the upcoming FIFA World Cup, America 250 celebrations, and the 2028 Olympic and Paralympic Games - fusion centers function as the primary hubs for consolidating threat information, coordinating across jurisdictions, and ensuring that actionable intelligence reaches decision makers and frontline agencies when it matters most. There is no substitute for the National Network of Fusion Centers – they fill a unique role that cannot be replicated by any one entity. Working together with the Intelligence Commanders Groups of the Major Cities Chiefs Association (MCCA) and the Major County Sheriffs of America (MCSA), and in collaboration with statewide investigative agencies that are part of the Association of State Criminal Investigative Agencies (ASCIA), fusion centers play an essential role helping to protect America.

Today, I will focus on how information sharing should function during major events, what we have seen work well in recent large-scale security operations, and where gaps remain - particularly in threat reporting, real-time coordination, staffing, training, and access to intelligence. I will also discuss the role of DHS I&A and other federal partners in supporting fusion centers in both steady-state operations and during major events, including the resources and authorities needed to ensure this system functions effectively in the years ahead.

**Major Event Preparation**

Major events such as the FIFA World Cup, America 250 celebrations, and the Olympic Games place extraordinary demands on the homeland security enterprise. These events are not single venue or single jurisdiction challenges. They extend across multiple cities, counties, and states well beyond the secured perimeter.

Threats associated with major events often emerge far from the venue and long before the event itself, surfacing through routine law enforcement encounters, online activity, and tips from the public. The scale and duration of these events test how well our information sharing systems work in practice, making real time, multi-jurisdictional coordination mission critical. Fusion centers exist to meet this challenge by consolidating tips and leads, integrating intelligence from multiple sources, identifying patterns across jurisdictions, and ensuring actionable information reaches the right partners in time to act.

**What Is Working**

When federal, state, and local partners are aligned in the field, our nation's information sharing apparatus works the way it was intended by the recommendations of the 9/11 Commission Report. When federal partners deploy alongside fusion center analysts and threat liaison officers with a shared mission and real time access to disparate sources of information, communication improves immediately. Intelligence products become more timely and relevant, questions are resolved more quickly, and operational decisions move faster.

The collaboration that occurred in my area of responsibility during and preceding Super Bowl LX, which happened in the City of Santa Clara, Santa Clara County, and included NFL events in the City and County of San Francisco, is a clear example of how the information sharing environment approach was intended to work. Sustained planning and real time coordination between the FBI, HSI, the U.S. Attorney's Office, and other Department of Justice and

Department of Homeland Security components, including the Office of Intelligence and Analysis (I&A) and the Cybersecurity and Infrastructure Security Agency (CISA), along with fusion centers, the Bay Area Urban Area Security Initiative (UASI), Center for Internet Security (CIS), and state and local public safety agencies, enabled integrated threat reporting and shared situational awareness. That coordination allowed partners to identify risks early, align protective measures, and respond quickly as conditions evolved.

For example, days before the Super Bowl, the Central California Intelligence Center (CICC) in Sacramento identified a subject that had shared on-line content indicating his intention to violate restricted air space during the game at Levi's Stadium with an Unmanned Aircraft System (UAS). The significance of the threat was that the subject had been convicted of violating the same restricted air space and dropping objects from a drone after entering Levi's Stadium on November 26, 2017. Thanks to CICC's swift action in passing the lead to the NCRIC, all the personnel that were protecting the venue were aware of the threat and law enforcement partners in Sacramento were able to mitigate the planned drone incursion by seizing the drone.

The night before the Super Bowl, the NCRIC team and our public safety intelligence and transportation security partners were briefed in the Super Bowl Regional Coordination Center (RCC) in the City of San Jose, on passenger rail sabotage threats related to the 2026 Winter Olympics in Italy by our CISA and I&A partners. The tactics, techniques, and patterns were quickly identified and a team of local, state, and federal analysts worked with our fusion center personnel to develop a bulletin that was quickly disseminated to front-line personnel from multiple agencies around the San Francisco Bay Area to increase awareness and improve the ability to detect and mitigate potential threats to the public.

During the weeks ahead of this month's Super Bowl, law enforcement and Non-Governmental Organizations (NGOs) worked together to fight against human trafficking and contacted 73 adult and 10 juvenile human trafficking victims, including a 12-year-old child, and offered the victims of sex trafficking support to escape their traffickers. Law enforcement also arrested 29 suspected human traffickers by the time the first whistle was blown on Super Bowl Sunday. The Santa Clara County Human Trafficking Task Force spearheaded the collaboration with over 60 partner agencies in 11 counties, with the support of NCRIC analysts.

By consolidating human trafficking data sources through an information sharing environment that combined the technologies from a common public safety Geographic Information System (GIS) analysis tool with a commonly used chat, video, and file sharing technology, analysts and officers were able to integrate tips, online threat indicators, field reporting, and investigators' requests for information across multiple jurisdictions. The fusion center analysts were able to identify patterns and support the joint investigative effort of the partner agencies with real – time analysis that would not have been possible through isolated reporting or other information sharing platforms.

**Persistent Gaps in Threat Reporting and Coordination**

Despite these successes, it is imperative that we improve how information sharing, information access, and analytical collaboration function when those functions must operate at scale and speed ahead of and during major events.

Threat reporting overall, despite improvements, remains fragmented. Tips and leads enter the system through multiple pathways - including local agencies, federal partners, private entities, venue security, and the public. But there is no single, reliable workflow to rapidly consolidate, deconflict, and disseminate that information across jurisdictions. During fast moving events, this fragmentation can undermine shared messaging and situational awareness.

At the same time, federal systems used by DHS and the FBI are not fully interoperable with state and local platforms. Agencies are often working from partial information, and critical data does not always reach the right analysts or decision makers in time, which means that front-line personnel who are best positioned to recognize, report, and respond to potential threats are less aware. During major events, these gaps are not theoretical, as during the Super Bowl, we had several information sharing platforms that operated at the same time. This creates an operational risk at large scale events and creates stress on an already overtaxed network of analysts and officers.

The upcoming FIFA World Cup highlights these challenges in very real ways. In some host regions, state and local law enforcement agencies are facing significant security responsibilities without clear coordination or operational alignment across all partners involved in the sprawling events from practice locations, team hotels, to official and unofficial events for fans. As a result, local agencies are not as connected as they should be for planning, staffing, coordination, and real time information sharing for a complex, multi-jurisdictional event.

For events of this scale, that approach means serious risks may go unaddressed. World Cup security is not confined to a single venue or jurisdiction; it extends across host cities and surrounding communities. Without clear coordination, defined roles, and aligned support, information sharing becomes more difficult, and local agencies whose resources are already stretched too thin, are left to manage complex, multi-jurisdictional threats under significant time pressure.

These challenges underscore why major international events require a coordinated, multi-jurisdictional approach that aligns federal, state, local, and private-sector partners around shared information, shared expectations, data security, and shared responsibility.

**DHS Office of Intelligence and Analysis**

Within the broader information sharing framework, the DHS Office of Intelligence and Analysis plays a unique and irreplaceable role. I&A is the only element of the U.S. intelligence community statutorily charged with facilitating intelligence sharing with state, local, tribal, and territorial partners, including the National Network of Fusion Centers, regarding terrorism and other threats to the homeland.

From our perspective in the field, I&A is most effective when it is forward-deployed with access to federal information and the authority to appropriately share it with state and local partners. I&A personnel embedded in fusion centers enable a timely two-way flow of information and the collaborative analysis and development of intelligence – increasing the likelihood that the reporting of threats reaches state and local partners quickly, while insights developed at the local

level inform the national intelligence picture. During major events, this field presence can determine whether threat-related information and intelligence arrives in time to help personnel on the ground recognize and prevent an incident, or whether it is too late to be useful.

In major urban areas that host major events, a single I&A representative is insufficient. Effective support requires that field teams have access to the right information and the authority to share that information and develop joint intelligence products with state and local partners. I was lucky enough to have the highest tier of support possible from DHS I&A during the Super Bowl, as they sent 14 members of their team from their Field Intelligence Directorate and Special Events Program to assist the NCRIC. Those forward-deployed intelligence analysts and officers must also be supported by a headquarters structure at I&A that is capable of sustaining and scaling those efforts for future major events and daily fusion center operations.

For these reasons, we are grateful that the Committee has included NFCA and our law enforcement partners in discussions on proposed legislative reforms to strengthen I&A's ability to support state and local law enforcement and all our communities. Stakeholder input is essential. Decisions about staffing, authorities, release processes, and coordination mechanisms directly affect whether intelligence sharing works under the compressed timelines and heightened risk of major events. Any reform effort should strengthen – not weaken – I&A's field presence and ensure it is backed by a robust headquarters enterprise with access to relevant information from other federal partners and the Intelligence Community and the authority to share appropriately with state and local partners including fusion centers.

**Drone Threats at Major Events**

Unmanned aircraft systems present a growing threat to both major events and everyday public safety. We appreciate Congress's action in December 2025 through the *Safer Skies Act*, which passed as part of the FY26 National Defense Authorization Act, which granted state and local law enforcement and correctional agencies the authority to detect, track, and mitigate malicious and unauthorized drones, subject to appropriate training and equipment requirements.

From the field perspective, the challenge now is implementation. Access to the FBI's required counter-UAS training is severely limited, and demand already far exceeds available capacity. As a result, many state and local agencies - particularly those preparing for major events - do not yet have trained personnel in place to operationalize this authority in a meaningful way. We are encouraged by the administration's intent to consult closely with state and local law enforcement and corrections as implementation of the *Safer Skies Act* begins this year. We encourage Congress to allocate the funding necessary to increase availability of FBI training for state and local agency personnel so we can take quick action to mitigate drone threats to our major events and every-day community safety.

Under the *Safer Skies Act* Congress also authorized the use of existing Justice Department grant programs, specifically Byrne JAG and COPS grants, to support the acquisition of drones for public safety missions and also counter-UAS systems. In addition, funding provided in the *One Big Beautiful Bill Act* through FEMA's State Homeland Security Grant Program supports law enforcement activities that include counter-UAS and other capabilities relevant to major event security. These tools are critically important, but they are not sufficient on their own. Counter-

UAS capabilities require sustained investments in training, staffing, equipment, and operational integration that exceed what these programs can support. I urge Congress to consider how the federal government can support state and local efforts to build and maintain robust drone first-responder capabilities and counter-drone operations to protect the public.

Addressing these gaps will require additional, flexible federal resources. Without that support, state and local agencies will continue to face challenges translating the new authority that Congress has provided into effective protection for our communities.

**Grants and Resources**

Federal grant programs play a critical role in enabling state and local agencies to contribute to the national security mission every day and to scale those capabilities for major events. These resources support the personnel, training, technology, and coordination that make timely information sharing and threat detection possible across jurisdictions.

Fusion centers and our state and local partners use programs such as the State Homeland Security Grant Program (SHSGP) and the Urban Area Security Initiative (UASI) to support analysts, training, analytical technology, and multi-jurisdictional exercises and coordination. These programs are central to local, regional, and national threat prevention efforts, yet agencies continue to take on expanding responsibilities and increasingly complex threat environments while planning and execution have been complicated by uncertainty around grant guidance, eligibility requirements, and the timing of fund disbursements that if not resolved soon, will hinder or derail national priority projects that have been designed to prevent and mitigate major threats to our nation.

Information sharing capacity does not scale up on demand without dedicated planning and resourcing. The analytical workforce and coordination mechanisms required for major events such as the FIFA World Cup, America 250 celebrations, and the Olympic Games must be built and sustained over time. Because threat actors routinely cross state lines and international borders, and because each part of federal, state, and local governments may have information, capabilities, or resources, the federal government has a responsibility to contribute funding and personnel to supplement and help sustain state and local capabilities. Delayed guidance or funding timelines directly affect readiness across the system.

As this committee considers homeland security and public safety priorities, it should ensure that FEMA preparedness grant programs provide predictable funding, timely guidance, and sufficient flexibility to support sustained information sharing capabilities across jurisdictions. These investments enable fusion centers and our partners to fully contribute to the homeland security and national security missions and ensure coordinated readiness for major national and international events.

**Cyber Threats**

Cyber threats may represent the greatest vulnerability surrounding major events because adversaries do not necessarily need physical proximity to cause harm. A successful cyberattack against power, water, communications, or transportation systems during a major event could create cascading effects that overwhelm response capabilities.

For major events, cyber threats underscore the need for real time information sharing well beyond the event's geographic footprint. Fusion centers often lack timely access to cyber threat indicators and trend data, and despite progress in recent years there is no fully integrated national approach to state and local cyber threat response. Fusion center and partner agency analysts also need continued DHS ITA Cyber Analyst Seminar and Webinar training, as well as advanced cyber analyst training.

Strengthening information sharing in this area will require better integration between federal cyber partners, fusion centers, and other state and local officials. It will also require clearer pathways for sharing actionable cyber threat information from federal entities to state and local agencies, and sustained investment in analytic capacity at the state and local levels. Without these connections in place, cyber risks associated with major events will continue to outpace our ability to detect and respond in time.

**Law Enforcement Tools and Investigative Technology**

Effective information sharing for major event security depends on access to a range of lawful tools and data - not a single technology. Fusion centers and their partners rely on investigative technologies, including commercially available data, to identify potential threats early, connect disparate data points, and support timely operational decisions before and during large-scale public events.

Tools such as automated license plate recognition (LPR), facial recognition, and social media open-source intelligence analysis support threat detection and situational awareness for planned and unplanned events. These tools help identify patterns and emerging risks early enough to share information across jurisdictions, enabling coordinated prevention and response efforts before harm occurs.

As Congress considers consumer data privacy frameworks, it is critical that any approach be developed in consultation with state and local law enforcement and account for the real-world public safety needs. Data privacy proposals could have a major impact on investigative efforts given the ubiquity of data across our world today. One of those proposals – the Fourth Amendment Is Not For Sale Act (FANFSA) – would force analysts and investigators who are trying to prevent harm and protect the public to be blind to information that others can readily access. That makes no sense from a public safety or homeland security standpoint. Efficient, timely, and privacy-protective sharing of digital evidence is essential. Legislative frameworks must preserve lawful access necessary for timely information sharing while maintaining strong privacy, civil rights, and civil liberties protections.

**Communications and Information Access**

Effective information sharing for major event security depends on reliable communications and timely system access. Fusion centers require access to local, regional, state, and federal information at both the classified and unclassified levels, including law enforcement records, criminal intelligence databases, the Homeland Security Information Network, the Homeland Security Data Network, FBI Criminal Justice Information Services systems, DHS law enforcement and screening systems, and tip and lead intake platforms.

This access allows fusion centers to add critical local context to national intelligence and support coordinated, multi-jurisdictional threat prevention efforts. During major events, delays or barriers to system access directly undermine situational awareness and slow decision making for personnel responsible for public safety on the ground.

Current federal platforms offer some functionality, but they remain limited in their ability to support real-time, large-scale coordination across agencies and jurisdictions. As Congress considers legislative reforms to DHS I&A and other federal components, any legislative or policy changes should ensure fusion centers retain timely, operational access to necessary systems and prioritize interoperability and real-time communications across jurisdictions that allow analysts and officers to enter the data once, instead of the several times that they have to enter the same data today into multiple systems. Without these capabilities, fusion centers are far less able to support major event security or rapidly share threat information before harm occurs.

**Security Clearances**

Timely security clearances are essential to effective information sharing during major events. Ongoing delays limit fusion center personnel's ability to access critical intelligence and fully participate in secure coordination with federal, state, and local partners.

During major events, personnel without timely clearances may be unable to access or share threat information or participate in secure coordination spaces, directly undermining joint situational awareness and response planning.

As Congress and the Administration consider reforms to personnel security and information sharing policies, I urge you to prioritize timely clearance processing and access for state and local fusion center personnel, including appropriate use of reciprocity and provisional access to meet time-sensitive operational needs.

**Closing**

The upcoming World Cup, America 250 celebrations, and Olympic Games will test the homeland security enterprise in ways we have not experienced in decades. Threat-related analysis and information sharing is not a supporting function for these events – it is an essential mission that must be developed and exercised routinely to protect our communities.

Fusion centers sit at the center of that mission, connecting federal intelligence with state and local operational response. When information sharing is timely, integrated, and properly resourced, threats can be identified and mitigated before they reach the public.

We appreciate the Committee's engagement and its inclusion of the NFCA in discussions on major event security, information sharing, and I&A reform. We stand ready to continue working with you to ensure our analytical and information sharing systems and practices are prepared for the challenges ahead.