



STATEMENT FOR THE RECORD

Mike Sena

President, National Fusion Center Association  
Director, Northern California Regional Intelligence Center

United States House of Representatives  
Committee on Homeland Security  
Subcommittee on Counterterrorism and Intelligence  
“State and Local Perspectives on Federal Information Sharing”

September 8, 2016

Mr. Chairman, thank you for inviting me to testify on this important topic. My name is Mike Sena and I am testifying today in my capacity as President of the National Fusion Center Association (NFCA). I am currently the director of the Northern California High Intensity Drug Trafficking Area (HIDTA) and Northern California Regional Intelligence Center (NCRIC), one of the 78 fusion centers in the National Network of Fusion Centers (National Network). Fusion centers bring together law enforcement, public safety, fire service, emergency response, public health, protection of critical infrastructure and key resources (CIKR), and private sector security personnel to understand local implications of national intelligence, and add state and local information and context to federal intelligence, thus enabling local, state, and federal officials to better protect our communities.

Since we last met in February of 2015, we have seen progress in the analysis and sharing of information related to threats to the homeland. We have also seen demonstrations of gaps that still exist. As I stated in my testimony last year, our public safety, law enforcement, and intelligence communities have made dramatic progress since September 11, 2001. This progress has not come without its roadblocks. As we continue to work through those challenges with help from this committee, we believe that we are on the right path and making steady improvement. At the end of the day, it's about meeting the needs and expectations of the American people that we keep them safe while respecting their rights.

At a high level, I believe we should be working toward the following four priorities to improve our ability to do that:

- 1) Strong federal support for fusion centers through SHSGP and UASI grant funding, and accountability behind the Law Enforcement Terrorism Prevention (LETP) requirement in current law.
- 2) Strong engagement by DHS, FBI, and other federal partners directly with fusion centers including the forward deployment of intelligence officers and analysts at fusion centers.
- 3) Strong training and network development between fusion centers, police chiefs, sheriffs, fire chiefs, rank and file, emergency management and other public safety partners at all levels of government and across all geographies to ensure tips, leads, suspicious activity, and criminal intelligence data are flowing efficiently for analysis and sharing.
- 4) Strong connectivity and direct engagement between federal, state, and local investigative and analytical entities with responsibility for cybersecurity.

Over the past year, we have seen the important role the National Network of Fusion Centers plays in supporting lead investigative agencies in the aftermath of horrific tragedies - both terror attacks and criminal activity - in Orlando, San Bernardino, Baton Rouge, and elsewhere. Immediately after the San Bernardino terrorist attack, analysts at the Joint Regional Intelligence Center (JRIC) were developing intelligence on suspects and sharing it directly with the San Bernardino Police Department, San Bernardino Sheriffs Office, and the FBI.

An alert sheriff's deputy who had recently received training at the JRIC called the fusion center to report that an individual matching the description of the person wanted in connection with providing weapons to the shooters was about to check out of an area hospital. The fusion center immediately passed the information to the task force that was about to launch a manhunt for the individual, enabling them to call it off before it even started. It may seem simple, but the fast and efficient flow of tips, leads, and intelligence products is challenging in practice. Fusion centers are at the forefront of removing

barriers, developing better pathways, and maintaining relationships that help information analysis and sharing happen faster. The JRIC's role after the San Bernardino attack is one clear example of that.

We have found after many of the recent high-profile terror attacks over the past year (San Bernardino, Paris, Orlando) that reporting of suspicious activity by public safety personnel and by citizens rose sharply immediately after the events. Some people send information directly to the FBI. Others don't know who to call, and naturally look to their local police agency or call 911. Thanks to an ever-growing network of liaison officers, those reports are routinely forwarded to fusion centers. Analysts vet those reports, provide local context around the information reported, and share information directly with the FBI via eGuardian.

I am still often asked whether fusion centers duplicate the FBI's JTTFs. This committee knows the difference, but many people are still not fully aware that JTTFs are federally run investigative bodies that support the FBI's unique mission to investigate terrorism threats in this country. Fusion centers play a much different role; they're not only information sharing hubs in states and metropolitan regions. Fusion centers are where we train a cadre of terrorism liaison officers (TLOs), including police officers, firefighters, EMS workers, and our private sector partners on indicators and warnings of terrorism. Fusion centers have the ability to catalogue critical infrastructure in each state and region and analyze incoming suspicious activity reports (SARs) against the national threat picture and against what we know about our critical infrastructure. We have the ability to rapidly share information and intelligence among the entire National Network and with the FBI. But often that SAR information has no nexus to terrorism. It's about drug dealing or gang activity or firearms trafficking or mortgage fraud. So the all-crimes approach mentioned above gives us the ability to analyze that information and funnel it to the right place. And we know that, sometimes, information that at first blush appears to be criminal in nature actually is linked to terrorist activity.

In the wake of serious ISIL-inspired threats to law enforcement and other public safety officers around the country, the NFCA worked closely with the FBI to prepare a "Duty to Warn" memorandum to fusion center directors and FBI field office executive management to advise them of certain protocols and assistance for identifying and warning individuals that are the targets of threats. We also worked with the FBI to produce additional guidance on deconfliction efforts between state and federal partners on the Duty to Warn documents.

An essential part of continued improvement is the Federal support provided to fusion centers. That Federal support includes assignment of intelligence officers and analysts, technical assistance, training and exercises, linkage to key information systems, grant funding, and security clearances. For

example, the FBI has assigned 94 personnel either full time or part time to 63 out the 78 fusion centers across the country. DHS has assigned 103 personnel to the fusion centers, including intelligence officers, regional directors, and reports officers.

The support of the Program Manager for the Information Sharing Environment (PM-ISE) and his office has been critical to some of the progress we have made since the last hearing. From continuing to coordinate the development of standards for sharing information across sectors, to enabling a single sign-on capability for personnel in fusion centers and other field-based information sharing entities to access multiple criminal intelligence databases, to paving the way for coordinated deconfliction of law enforcement operational events across multiple systems, the PM-ISE and his staff have been essential partners of ours. Another PM-ISE supported project is currently underway with the Northeast Regional Intelligence Group (including all of the fusion centers in the Northeast region) that will result in deeper cooperation and coordination among information sharing entities and a wider set of public safety partners in the region. The ISE annual report for 2016 was just published, and I strongly encourage members of this committee to visit the ISE website and review that report for more background on the progress we are all making together.

These resources add critical value to the resources committed by state and local governments to make the National Network a foundation of homeland security information sharing. Over the past several years, the state and local share of budget resources allocated to fusion centers has grown substantially - state and local governments provided well over half of all funding for fusion centers in FY 2015. In addition to concrete personnel and financial resources, the dedication of time and deliberate effort to continually deepen engagement with our federal partners has been critical. One recent example of this was past month when personnel from 14 fusion centers participated in a weeklong forum at FBI headquarters to exchange information regarding best practices in analytical collaboration and information sharing between the FBI, other federal partners, and the National Network of Fusion Centers.

### **Addressing Ongoing Challenges**

Since fusion centers are separately owned and operated by state and local entities, there is variation among the centers in terms of budget and capabilities. That variation in capabilities has an impact on the expectations of our local, county, state, and federal public safety partners and customers. To address this, the NFCA has initiated an effort to formalize a standard process for collection of analytical tradecraft best practices and operational success stories. We are also working to establish a single virtual location for these best practices so that anyone who is part of the National Network of Fusion Centers

- from new directors to analysts - has a “one-stop shop” for resources to help improve their capabilities and understand what is happening across the National Network. We are creating new opportunities for advanced training for fusion center analysts, including collaborating with our federal partners on advanced analyst training. There is currently no broadly accepted method for exchanging requests for information (RFIs) across the National Network of Fusion Centers and among our law enforcement partners at all levels. So we are working to standardize that process for exchanging RFIs through HSIN. Next month we will hold our annual conference in Alexandria, Virginia and will have representatives from nearly all fusion centers, all of our federal partners, and personnel from police departments, sheriffs offices, and other public safety entities around the country. We encourage members and staff from this committee to attend that conference to see up close the challenges we are addressing and the level of collaboration that has become routine.

We are continuing to address obstacles to progress in information sharing and analytical capabilities. For example, we have consistently called for more TS/SCI clearances for appropriate fusion center personnel. Without those clearances, the types of information our people are able to factor into their analysis can be inadequate. In some cases, sensitive information that should be shared by federal partners is not shared. We also believe that the FBI should explore the inclusion of fusion centers in its threat review and prioritization (TRP) process to ensure a more complete understanding of the threats facing our nation. In addition, we have voiced strong concerns about the chilling impact of Freedom of Information Act (FOIA) interpretations on the willingness and legal ability of state and local law enforcement entities to share certain state and locally derived information and intelligence with our federal partners. Also, we need to create standards related to “law enforcement sensitive” (LES) information. Currently there is no official designation of LES as a classification category and no penalties for unauthorized release of LES information. If we want to share certain types of threat information with a broader public safety audience for their situational awareness and security resource decision making, it cannot be at the “Secret” level. It has to be FOUO/LES, which can still reveal sensitive information about ongoing investigations and jeopardize those cases. Yet there is no way to enforce or penalize violations.

Finally, we have been working hard over the past several months to address the current inability of several fusion centers to obtain access to certain federal criminal justice information databases through FBI CJIS. In my mind it is unacceptable that some state and local entities whose mission clearly includes providing support to investigative agencies on criminal threats cannot get access to data sets that are fundamental to good analytical work. It is a clear obstacle to information sharing and analysis up and down the chain, it is a glaring gap, and it should be remedied as soon as possible.

We are working with the FBI on an “enhanced engagement initiative” to ensure the FBI continues to improve its sharing of relevant counterterrorism information with fusion centers, while also enhancing the contribution of information and analysis from fusion centers in a coordinated and efficient manner to address the growing terrorism threat. We are working closely with our partners at DHS, the Program Manager for the Information Sharing Environment (PM-ISE), and the Criminal Intelligence Coordinating Council (CICC) on this project.

To facilitate situational awareness and share information across agencies about cyber threats, the NFCA Cyber Intelligence Network (CIN), which is a relatively new network of fusion center cyber analysts, tries to ascertain whether the intelligence developed in various states may be part of a broader trend. The CIN is comprised of over 250 federal, state and local law enforcement members who focus on cybercrimes. These members come together and act as a Virtual Fusion Center utilizing a cloud service provided by the Homeland Security Information Network (HSIN) to share real time cyber threat intelligence in support of an incident, event or mission. This level of cyber threat information sharing was impossible only a few years ago, yet now is becoming routine. Testimony by Lt. Col. Dan Cooney of the New York State Police before this committee back in May laid out several examples of how fusion centers are part of this effort. In May of 2015, the “Cyber Integration for Fusion Centers” Appendix was added to the Baseline Capabilities for State and Major Urban Area Fusion Centers guidance. Clearly, good progress has been made. But we are nowhere near where we need to be on cyber analysis and information sharing across all public safety jurisdictions. It should be a priority in the next presidential administration and in the next Congress to focus on this challenge.

We appreciate the work that this committee has done during the 114th Congress to ensure that fusion centers have the necessary resources to carry out their missions. The House of Representatives has approved multiple bills that originated in this committee to strengthen information sharing practices and more clearly define roles and responsibilities. We strongly encourage the Senate to consider those bills and act as soon as possible.

Mr. Chairman, on behalf of the National Fusion Center Association, thank you for inviting me to testify today. I commend you for your focus on this topic. It should continue to be a high priority for this committee and for all of Congress - especially in this dynamic threat environment. We look forward to continuing to work closely with the committee.