Statement of

Mike Sena

President, National Fusion Center Association

Director, Northern California Regional Intelligence Center (NCRIC)

Joint Hearing of the Subcommittee on Emergency Preparedness, Response, and Communications; and the Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies

Committee on Homeland Security
United States House of Representatives

"Cyber Incident Response: Bridging the Gap Between Cybersecurity and Emergency Management"

October 30, 2013

Chairman Brooks, Chairman Meehan, Members of the Subcommittees,

My name is Mike Sena and I am the Director of the Northern California Regional Intelligence Center (NCRIC), which is the fusion center for the San Francisco Bay and Silicon Valley region. I currently serve as president of the National Fusion Center Association (NFCA). On behalf of the NFCA and our executive board, thank you for the opportunity to share our perspective on the analysis and sharing of information on threats from the cyber domain that we are seeing at a rapidly increasing pace.

The National Network of Fusion Centers (National Network) includes 78 designated state and major urban area fusion centers. Every center is owned and operated by a state or local government entity. The majority of operational funding for fusion centers comes from state or local sources, while federal grants – primarily through the Homeland Security Grant Program at FEMA – are a major source of additional support. Our centers are focal points in the state, local, tribal, and territorial (SLTT) environment for the receipt, analysis, gathering, and dissemination of threat-related information between the federal government, SLTT, and private sector partners.

As the report on fusion centers that was released in July of this year by the majority staff of the full House Homeland Security Committee noted, nearly 200 FBI Joint Terrorism Task Force investigations have been created as a result of information provided to the FBI through fusion centers in recent years, and nearly 300 Terrorist Watchlist encounters reported through fusion centers enhanced existing FBI terrorism cases. Most fusion centers are "all-crimes" centers, meaning that they do not focus on just terrorism-related threats. Most centers are supporting law enforcement and homeland security agencies in their states and regions through analysis and sharing of criminal intelligence to address organized criminal threats and to support intelligence-led policing.

Because the National Network of Fusion Centers has developed into a mechanism for regular exchange of criminal intelligence and threat information across jurisdictions, we are increasingly involved in addressing cyber threats. My center – the NCRIC – is actively involved in cyber threat analysis and information sharing with our federal partners, other fusion centers, state and local governments in our region, and private sector partners. As with any other successful law enforcement or intelligence effort, good relationships are at the heart of the matter. We must develop strong and trusting relationships with our customer agencies as well as with the private sector to ensure timely information flow. As an example of partnership development, the NCRIC is working with a major utilities service provider - that faces significant persistent cyber attacks - to assign personnel inside the fusion center. Once in place, this partnership will result in the development of capabilities to improve internal security for the company, but also new threat analysis and prevention capabilities for other critical infrastructure partners across the sector. The NCRIC hosts a working group including private sector CIKR owners that meets regularly to discuss threats and share information.

But my center is not the norm across the National Network. Today, less than half of the fusion centers have a dedicated cyber program. We expect that number to grow as the threats grow, but we must have additional resources to support the specialized training and personnel to further that mission. We cannot take away from our established missions to tackle new ones. We also must coordinate

closely with other entities that play roles in cyber threat awareness, analysis, and information sharing – including the organizations my fellow panelists here today represent.

The reality is that we are dealing with a growing category of criminal activity featuring different impacts as compared to traditional crime. Because the impacts are "quieter" and – to date – most often bloodless, it is more difficult to make a clear case for investments in systematic improvements in law enforcement and criminal intelligence capacity to deal with these threats.

But as we all know, the threats and their consequences are very real. And the threats are growing – from small, targeted operations that impact a family's finances to large operations that threaten an electric grid. Large critical infrastructure owners know who to call when something happens – they are likely to have existing partnerships with federal law enforcement and investigative bodies. But who does a family call when they notice they have been violated? What about a small business or, even more concerning, a smaller vendor that may be part of an important supply chain? State and local law enforcement across the country are reporting increased calls related to cybercrime. Questions related to jurisdiction and investigative capacity are difficult to answer in many of these cases. But the analysis and sharing of threat information is essential to prevent more victimization.

As the NFCA has worked with our partners in state and local law enforcement on this issue over the past year, it has become clear that we have significant needs for capability and capacity enhancements. As I wrote in a blog post for the Program Manager for the Information Sharing Environment (PM-ISE) last week, the NFCA is working with the International Association of Chiefs of Police (IACP), the PM-ISE, private sector partners, and other professional associations to assess needs across the country. I want to specifically acknowledge the office of the Program Manager for the Information Sharing Environment, DHS Intelligence & Analysis, and FEMA for their recognition of the importance of this effort, and for moving the ball downfield. These are outstanding partners in our efforts and we rely on them daily.

In August 2012, the NCRIC hosted a roundtable for cybersecurity stakeholders that included representatives from the financial and IT sectors, as well as federal, state, and local officials. These participants identified two types of information sharing: 1) fusion centers engaged in sharing tactical information on company or sector-specific situational awareness; and 2) fusion centers sharing strategic information on threats, risks, and trends through strategic forums that involve both the public and private sectors. IACP partnered with the Department of Homeland Security to facilitate a December 2012 roundtable to further clarify requirements for cybersecurity information sharing.

Building on the momentum of the August and December events, the NCRIC and the IACP held the Cybersecurity Evaluation Environment Pilot Kick-off Event in February 2013. The first day of this two-day event focused on soliciting cybersecurity information sharing requirements from industry partners and developing potential federal, state, and local government processes for cybersecurity information sharing with the private sector. Participants also discussed government requirements for cybersecurity information sharing. On the second day, the government participants worked to design a "cybersecurity pilot" that would advance fusion center cybersecurity information sharing capabilities.

The pilot will be funded by DHS through the Multi-State Information Sharing and Analysis Center (MS-ISAC) and executed in coordination with all appropriate stakeholders. It will focus on addressing needs identified by stakeholders including:

- the need for increasing the timeliness, volume and the quality of the information the federal government shares with state/local/tribal government and private sector partners;
- the need for standardization of information sharing processes between the federal and state/local/tribal governments and the development of cyber response best practices;
- leveraging current counterterrorism-developed tools and processes for cyber incident handling and intelligence sharing;
- enhancing the protection of state/local/tribal networks
- supporting cyber crime investigations; and
- promoting private sector cooperation and information sharing.

We expect the pilot to get underway soon and we look forward to keeping the committee apprised of our actions.

We believe it is important to recognize a couple of realities. First, a streamlined system for reporting, analyzing, and sharing threats and incidents requires leadership at the state level in each of our states and a clear acceptance of what roles fusion centers can and should play. Roles, responsibilities, and capabilities should be clearly understood – including by private sector partners – and we have to acknowledge that we are not where we need to be. That is why efforts like the pilot project we are about to engage in with the leadership of PM-ISE and IACP are so important. While the systems of interaction may vary from state to state, we need structured relationships so that our personnel know where information should be flowing from and disseminated to.

Second, our human resource base in investigative and intelligence settings at the state and local levels has not adapted quickly enough to address the increased cyber threat. Again, citizens report crimes to law enforcement no matter the type. Federal agencies cannot possibly investigate all of those crimes, even as they have a need to be aware of them in case they relate to other incidents in other locations. State and local law enforcement, homeland security, and emergency management functions – including fusion centers – must be resourced to respond to those crimes quickly and share information rapidly so that additional crimes can be prevented.

As the July, 2013 committee staff report on fusion centers noted, "Ultimately, it is the FBI's responsibility to conduct counterterrorism investigations. However, no single government entity has the mission and capacity to coordinate, gather, and look comprehensively across the massive volume of State and locally owned crime data and SARs and connect those 'dots', particularly those related to local crime and, potentially, the nexus between those criminal activities and terrorist activity. This is the principal value proposition for the National Network." This reality extends to the cyber threat domain.

Next week the National Fusion Center Association will host a major event across the river in Alexandria, Virginia. The NFCA Annual Training Event will bring together fusion center directors and

analysts from nearly all 78 centers, as well as federal partners including DHS, partner associations from state and local law enforcement and emergency response, fire service representatives, and industry to receive training and share best practices. Among the training sessions are two separate sessions on cyber threat analysis and information sharing. Representatives from the Kanas City Terrorism Early Warning Group, the Orange County (CA) Intelligence Assessment Center, the Louisiana State Analytical and Fusion Exchange (LA-SAFE), the San Diego Law Enforcement Coordination Center, and my center – the NCRIC – will present to other fusion centers on effective practices and partnerships they are implementing in their centers. This indicates the level of interest across the National Network in advancing our capabilities to address cyber threats.

The state of Louisiana's fusion center – LA-SAFE – has taken an active role in cyber threat analysis and information sharing. State, local, and private entities reach out to LA-SAFE when a cyber event occurs in their AOR. The fusion center's lead cyber analyst disseminates block-list information to those partners to quickly help strengthen their protections. LA-SAFEconducts analysis of cyber threats and develops intelligence reports for dissemination to relevant partners. To date, the LA-SAFE Cyber Unit has developed more than 40 reports that have been shared with federal, state, and local partners. Feedback to LA-SAFE – including from our federal partners – clearly indicates that the information coming out of the fusion center is of high value.

In one example from earlier this year, the Louisiana state legislature was receiving numerous phone calls from a foreign individual asking for the payment of a supposed debt. The numerous malicious calls clogged the phone-lines, preventing legitimate calls from going in or out. The "telephone denial-of-service attack" disrupted the legislature's communications. LA-SAFE determined that this TDOS attack was similar to others that had occurred across the United States and produced and disseminated an advisory to its partners. Immediately afterwards LA-SAFE received numerous phone calls and emails from public safety answering points (PSAPs) across the country that had suffered similar attacks. LA-SAFE was contacted by the Deputy Manager of the National Coordinating Center for Communications (NCC). The NCC had received the LA-SAFE advisory from the NCCIC and expressed serious concern. The NCC then initiated a conference call with LA-SAFE, the NCRIC, NCC, NCCIC, Association of Public-Safety Communications Officials (APCO), National Emergency Number Association (NENA), FBI and other industry representatives to coordinate a response.

As a result of the coordination, multiple advisories were distributed from participating organizations to their customer bases. It has since been determined that over 200 of these attacks have been identified nationwide. These attacks have targeted various businesses and public entities, including the financial sector and other public emergency operations interests, such as air ambulance, ambulance and hospital communications.

This example of cyber threat analysis and information sharing is occurring on a more frequent basis across the National Network of Fusion Centers. Some fusion centers are collecting and analyzing instances of cyber attacks in their AOR, and developing products that are sent to other fusion centers, which enables a much larger set of stakeholders to prevent damaging attacks.

LA-SAFE's recent experiences demonstrate both the opportunity and the need for additional focus and capacity within the network. Like other fusion centers that provide cyber threat analysis and sharing services, LA-SAFE needs more cyber analyst positions. The increasing threat level has already translated into increased demand for investigative and analytical services from fusion centers, and there is no sign of any slowing-down in that demand. A significant challenge for LA-SAFE and other centers is that cyber analysts are typically more expensive than traditional analysts. While physical terror threats and criminal activity are the primary focus of most fusion centers, the growing category of cyber crime means that cyber threat analysis resources must be strengthened at all levels of government.

In addition, LA-SAFE and other centers believe that the system for interacting with federal partners on cyber threats needs to be improved. Enhanced cooperation by federal partners through more information sharing at the unclassified or sensitive-but-unclassified levels would help connect dots and lead to faster information sharing to prevent attacks. Our federal partners tend to operate on the "high side," but since threat information is coming to fusion centers from state, local, and private sector customers who expect timely responses, operating in a classified environment can slow down information flow. Speed is important in all investigations and prevention activities – especially in the cyber domain. We must work with our partners to identify the right path forward on classification so that we can be appropriately responsive to our communities while safeguarding CIKR and information assets from inappropriate exploitation.

Building, training, and maintaining a strong cyber analyst cadre within fusion centers and law enforcement entities should be a priority. We have great partners like the United States Secret Service whose Hoover, Alabama training facility provides beginning and intermediate training for fusion center and other analysts. That program should be prioritized for new investment in the immediate future so that its training can reach a greatly expanded audience. The Multi-State Information Sharing and Analysis Center (MS-ISAC) provides training to state and local law enforcement to enhance cyber awareness and analytical capabilities. We need more of this type of training to ensure our analysts have the skills required to act quickly so that accurate, timely information can be shared broadly.

The Terrorism Liaison Officer (TLO) program is a successful partnership between fusion centers and the state and local law enforcement, first responder, public health, and private sector communities within their AORs. TLO programs train thousands of individuals on indicators of possible terrorist activity and reinforce a system of reporting of suspicious activity through the fusion centers and the Nationwide Suspicious Activity Reporting (SAR) Initiative. This system maximizes situational awareness and provides a clear mechanism for ground-level suspicious activity to quickly funnel up to lead investigative agencies.

The success of the TLO program in the physical terrorism domain should be extended to the cyber domain in the form of a "cyber TLO" program. Trained TLOs know what to do in the world of physical threats. The same should happen with cyber threats. City governments, county governments, state governments, and CIKR owners and operators should be part of this network. Again, maximizing situational and threat awareness through a systematized reporting mechanism will ensure that

investigative leads filter up to lead investigative agencies, while regular reporting on the latest cyber threats by fusion centers and other partners can be pushed down through that network.

Every fusion center should have the ability to triage threat reports and develop products to help state, local, and private sector entities to mitigate the threats. Ideally, we need a constantly updated automated system that provides partners information – machine and human-readable – in real-time as events are happening. Investigation into the source of cyber attacks will occur after the fact, but action to identify the attack, identify the associated indicators of compromise, and disseminate those indicators of compromise to partners in a timely manner is essential.

It will take time and money for that vision to be realized – and we have too little of both in the near term. In the meantime, the partners at this table and around the country must work together through the pilot project and other settings to develop policies, protocols, and requirements that will result in the kind of information sharing and threat analysis our citizens expect. In addition, a concept called analytical centers of excellence is being built out across the National Network. If a particular fusion center does not have dedicated cyber capabilities, then that center's personnel should know exactly where to go for support. Relationships should be developed and formalized so that centers with cyber capacity can be tapped when needed by other members of the National Network. This same concept is being applied to traditional criminal intelligence information by fusion centers today.

On behalf of the National Fusion Center Association, thank you again for the opportunity to testify today. The members of the NFCA executive board and I are happy to provide you with ongoing input and answer any questions you have. I also encourage you to reach out to the fusion center in your state or region and find out about their particular challenges and best practices related to cyber and other threats. We look forward to working with you on this issue.