



STATEMENT FOR THE RECORD

Bryan Costigan

Director, Montana Analysis and Technical Information Center
Supervisory Agent
Montana Department of Justice
Division of Criminal Investigation
Secretary, National Fusion Center Association

United States Senate
Committee on Homeland Security & Governmental Affairs
“Securing the Border: Assessing the Impact of Transnational Crime”

March 24, 2015

Chairman Johnson, Ranking Member Carper, thank you for inviting me to testify on this important topic. My name is Bryan Costigan and I am testifying today in my capacity as the director of the Montana Analysis and Technical Information Center (MATIC), one of 78 fusion centers in the National Network of Fusion Centers (National Network). Fusion centers bring together law enforcement, public safety, fire service, emergency management, public health, protection of critical infrastructure and key resources (CIKR), and private sector security personnel to understand local implications of national intelligence, as well as add state and local information and context to federal intelligence, thus enabling local, state, and federal officials to better protect our

communities. I also serve as Secretary of the Executive Board of the National Fusion Center Association (NFCA).

Information Sharing and Analysis Regarding Threats in Montana and Along the Northern Border

As my colleague Mike Sena, the president of the NFCA, indicated last month in testimony before the House Homeland Security Committee, our public safety, law enforcement, and intelligence communities have made dramatic progress over the past decade in analyzing and sharing information related to threats to the homeland. Information sharing on these threats - both criminal and terrorist in nature - has become more routine. Relationships have been developed and sustained across state and agency lines that are helping investigators solve crimes and prevent further crimes. Technology has given us better tools to support the process of analyzing and sharing threat information, and enhancing situational awareness during critical incidents. Federal support has been essential, including the assignment of intelligence officers and analysts from Federal partners, technical assistance, training and exercises, linkage to key information systems, grant funding, and security clearances. These tools add critical value to the resources committed by state and local governments to make the National Network a foundation of homeland security information sharing.

As Director of the Montana fusion center I can say that this improvement is evident on the Northern Border. While much of the country's attention is focused on the Southern Border, the vast expanse of our Northern Border presents countless opportunities for transnational criminal organizations and terrorist groups. Going forward, Congress should ensure that law enforcement and homeland security partners along the Northern Border at every level - including Border Patrol, Customs, Homeland Security Investigations, Immigration and Customs Enforcement, state, local, and tribal law enforcement - have resources adequate to meet the threats.

The State of Montana has 563 miles of border with Canada that spans two Border Patrol sectors and 15 ports of entry, including one in Glacier National Park. As long as I have been in law enforcement in Montana - more than 30 years - we have enjoyed a relatively strong culture of sharing resources among state, local, tribal, and Federal law enforcement agencies. It is not uncommon to have a variety of agencies responding to critical incidents along the border. There is an implicit understanding that each agency will support others. As this committee knows, it is often the cultural barriers to information sharing and coordination of analytical activities that prevent effective coordination. As I have had the opportunity to travel around the country as part of my responsibilities on the board of the NFCA, I have seen great improvements, but I also know there is much to be done. Leadership is the key ingredient in advancing the

effectiveness of our efforts. I am fortunate that my leadership in Montana - from Governor Bullock, Attorney General Fox, Division of Criminal Investigation Administrator Lockerby, and Investigations Bureau Chief Strandell - continually emphasize the need for collaboration to achieve our mission.

The Montana fusion center serves a focal point for information sharing among the many agencies that operate in the state. Within the center DHS is represented along with state and local agencies. The Joint Terrorism Task Force (JTTF) is located in the same state facility as the MATIC and that physical proximity enhances information sharing among agencies. In addition to our partners at MATIC we have shared information with the Border Patrol and Customs and Border Protection, as well as with Canadian agencies through CBP and Border Patrol partners at the Integrated Border Enforcement Teams (IBET). Our fusion center has completed joint products with DHS I&A, FBI, and CBP regarding issues that impact the border.

Drug trafficking organizations in Montana utilize well-established corridors that for the most part originate along the Southern Border. However, the rapid development of the Bakken shale oil region in Montana, North Dakota, and Saskatchewan has led to a major increase in illegal drug activity across our state. The oil boom has also brought a change in the players involved in drug trafficking through Montana. Previously, Montana-based organizations controlled much of the trade, and many Montanans would leave the state to procure larger drug quantities. Now we are seeing outsiders move into the trade to take advantage of the burgeoning population with more disposable income. A significant amount of methamphetamine used to be manufactured within Montana, but a combination of Federal and state policy initiatives and aggressive drug enforcement has caused a change in the illegal trade - over the past 10 years there has been a shift to smuggling finished meth from Mexico. Once rare in Montana, Mexican-sourced heroin is becoming more common as it competes with and beats in price the easily available opioid pharmaceuticals that are often the “gateway” to addiction. The majority of the non-marijuana illegal drugs in Montana utilize smuggling routes that originate in Mexico.

At the fusion center we are working with our state, local, and Federal partners including the Rocky Mountain HIDTA and other regional HIDTAs to analyze and understand these trends and provide information to support counter-drug operations. We are able to identify smuggling routes through coordination with investigators across the state by sharing analysis. In addition, access to reporting by federal agencies within classified and non-classified systems, reporting from HIDTAs such as Director Kempshall’s, the Regional Information Sharing Systems (RISS), and other fusion centers is critical. Very recently DHS shared information with our fusion center regarding an organization smuggling narcotics from Mexico through the United States into Canada utilizing Montana Ports of Entry. Utilizing this information, we are able to reach to our

state and local law enforcement partners to educate them on the organization's tactics and improve the ability for them to share information back with us and our federal partners to address the threat.

Elsewhere along the Northern Border, the Ohio Strategic Analysis and Information Center (SAIC - the Ohio state fusion center) is the hub for coordination for the Ohio Northern Border Initiative Task Force. The task force's mission is to provide law enforcement support in collaborative efforts with border partners to detect, deter, and respond to threats to the security of Ohio's international border, coastline, and inland connected waterways. The task force also interacts regularly with the Northeastern Ohio Regional Fusion Center in Cleveland. All of the county leads on the task force hold secret clearances and attend monthly briefings in Columbus at the SAIC. The task force also interacts regularly with the New York State Intelligence Center (NYSIC - the New York State fusion center) regarding foreign flagged vessels that have also travelled New York waterways.

In Maine, the Maine Information and Analysis Center (MIAC - the Maine state fusion center) is engaged daily with federal partners on border security efforts. In fact, a CBP officer is assigned to the MIAC and works in the fusion center's space, so collaboration on joint efforts related to the Northern Border is occurring on a daily basis.

In 2012, a South Dakota law enforcement officer encountered two foreign nationals at a traffic stop who were in possession of over 100 stored value cards and a credit card reader. This raised suspicions because criminal organizations are known for stealing credit cards or credit card numbers and transferring money from them to stored value cards. Since CBP requires that individuals declare monetary instruments totaling \$10K or more to Port of Entry Officials, criminal elements exploit a vulnerability in border security by using stored value cards because they can hold as much value as the vendor will allow and are easy to hide. The South Dakota officer sent a report on the individuals and their vehicle to the South Dakota Fusion Center (SDFC). After conducting state and federal records checks in coordination with the North Dakota State and Local Intelligence Center (NDSLIC) and Federal partners at ICE, it was discovered that the individuals had ties to an active ICE transnational organized crime money laundering investigation involving stored value cards. It was also discovered that the individuals had previously unknown ties to North Dakota, Washington, and Florida. Through this collaboration, the SDFC and NDSLIC were able to provide previously unknown information about the individuals to ICE to further support their investigative efforts.

In Michigan, the Michigan Intelligence Operations Center (MIOC - the Michigan state fusion center) coordinates with CBP, Border Patrol, and HSI on a regular basis to provide information and analysis pursuant to requests related to border threats. Recently, police in Windsor, Canada notified the Detroit Police Department that the Detroit/

Windsor tunnel would be shut down in both directions due to explosive devices found inside a vehicle. Multiple fireworks, knives, and other weapons were found and two male U.S. suspects were referred for secondary inspection by CBP. Analysts at the Detroit and Southeast Michigan Information and Intelligence Center (DSEMIIC - the regional fusion center in Detroit) assisted by providing complete work-ups for both suspects and provided the information to Border Patrol, DHS, and the Detroit Police Department, and the suspects were subsequently arrested.

Earlier this year CBP received information regarding a port runner into Canada. The subject's name and description was provided to DSEMIIC analysts, who provided a driver's license photo to assist law enforcement in locating the suspect. The suspect was apprehended by Windsor Police through a coordinated effort by DSEMIIC, CBP, Canadian Border Services Agencies, and Windsor Police. Last year, DSEMIIC analysts assisted the HSI BEST Detroit division on an Ecstasy smuggling ring from Windsor, Canada into the U.S. by providing vital records information, bridge cards, and affiliates of a total of 13 subjects. Analysts were able to identify associates of the subjects possibly involved in drug trafficking between Windsor and the U.S.

These stories are just a few examples from the Northern Border region of how fusion centers are serving as focal points for state and local analytic resources to support a variety of Federal Homeland Security missions beyond terrorism. Fusion centers regularly support DHS component agency investigative activities and on many occasions support disaster operations such as during Super Storm Sandy. Fusion centers routinely provide analytic support and information to United States Secret Service and HSI investigations into matters such as the proliferation of fraudulent Resident Alien Cards. My fusion center in Montana recently participated in a multi-state joint analytical effort with CBP regarding fraudulent drivers licenses, which can facilitate a range of criminal activity with obvious implications for border security. It is critical for Congress to recognize that fusion centers support the full spectrum of Homeland Security missions at the state and local level. Some DHS component agencies currently have personnel assigned to some fusion centers, and that level of engagement enhances information sharing and analytic collaboration. Border security is one of those Federal missions where fusion centers could be more effectively utilized to coordinate state and local resources to further enhance what is inherently a Federal responsibility.

The National Network of Fusion Centers

Thanks to strengthening partnerships across jurisdictional lines, we are sharing *more* information *more effectively* than ever before through fusion centers about a range of threats. This is happening despite the fact that no single entity has the authority to enforce effective information sharing practices. Because of the decentralized nature of

public safety in America, policies on sharing information - including information on threats that are related to our borders but are not stopped at the borders - cannot be dictated by any one organization. Common policies and practices have been developed by consensus through multilateral and interagency policy bodies - including the Global Justice Information Sharing Initiative (Global) and the Criminal Intelligence Coordinating Council (CICC) and must be continually reinforced through day to day engagements between Federal, state, and local partners. As you might imagine, this is extraordinarily difficult to achieve in practice, but we have made excellent progress and are continuing to build on that progress.

But we must work every day to overcome challenges related to jurisdiction, culture, security clearance levels, and information access if we want to continue to make progress. In my capacity as a board member of the National Fusion Center Association I am part of discussions nearly every day with my fusion center colleagues, our federal partners including the DHS Office of Intelligence & Analysis, our counterparts in other public safety disciplines, and with private sector stakeholders to develop stronger processes and build stronger relationships. With the active support of this committee and the rest of Congress and our state legislatures, we must continue our commitment to a true nationwide information sharing enterprise with the National Network of Fusion Centers as a centerpiece and build on the success we have achieved to date.

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 over half of all funding for fusion centers in FY 2014. Yet Federal funding support through FEMA Preparedness Grants - SHSGP and UASI - remains critically important. The NFCA has joined other law enforcement associations on a letter to Congress urging that the Law Enforcement Terrorism Prevention Activities (LETP) requirement in the Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53) be strengthened. The law requires that 25% of SHSGP and UASI funding be used for “law enforcement terrorism prevention activities” and specifies some of those types of activities including support for fusion centers. While states have latitude to allocate funding according to risk and priorities, we agree with the intent of the 2007 law and believe that terrorism prevention activities should be constant priorities, especially as grant funds have declined over the past five years. The Government Accountability Office (GAO) found in its November 2014 report on information sharing and fusion centers that in 2012 states inaccurately categorized about \$60 million in projects as “related to fusion centers” when in fact those funds did not support fusion centers. As we have suggested in our letter to Congress, requiring a governor-designated state law enforcement executive to review the LETP portion of grant plans would help to ensure those funds truly support terrorism prevention activities.

A common misconception that is often repeated in news stories and in advocacy papers is that fusion centers are “DHS fusion centers”. This is simply not true: DHS does not exercise operational control of any fusion center. State and local governments own and operate fusion centers, and we collaborate closely with DHS, the Department of Justice, and other federal agencies to facilitate wider analysis and sharing of threat information. Each governor designates a primary fusion center in each state. Together with other recognized fusion centers, these centers comprise the National Network of Fusion Centers. The national network is a decentralized, distributed network of analysts, public safety partners, and in a growing number of cases CIKR and private sector partners. Most centers have representation from DHS and in some cases the FBI and other Federal investigative agencies. This organizational structure allows for each center to be directed according to the priorities of its agency sponsor, while maintaining a direct upward and downward link to national counterterrorism intelligence. This is squarely in line with what the 9/11 Commission called for in its report.

Since fusion centers are owned and operated by state and local entities, there is wide variation among the centers in terms of budget and capabilities. Fusion center priorities in San Francisco are different from priorities in New York State and from our center in Montana. The interests are different because their populations, critical infrastructure, and threats are different, and the fact that they are free to address the issues they feel need to be addressed is a real strength of the national network of fusion centers.

The first of two common threads through all the centers – and the key Federal interest – is a link to Federal partners and to each other through information sharing mechanisms. The Critical Operational Capabilities (COCs) that are maintained (and measured through an annual assessment process facilitated by DHS) in each center ensure the centers are ready and able to support homeland security missions regardless of their local priorities.

Of central importance is the access each center has to local, regional, and state sources of information - public safety records, criminal intelligence databases, and personal relationships across communities - that allow the center to add local and regional context to national intelligence, as well as provide information and value-added intelligence to support counterterrorism and other criminal investigations that would otherwise be difficult or unlikely for lead Federal investigative agencies to obtain. Also critically important from the national perspective is that each fusion center has methods of distribution across local, regional, and statewide technical and personal networks that Federal investigative and intelligence agencies could not possibly build or maintain.

Thus, the dual value proposition of the National Network of Fusion Centers is that no other organizational structure can provide faster or more efficient access to state and local information that may support counterterrorism or other investigations, or enable

faster or more efficient situational awareness across relevant jurisdictions. Refining the processes that allow this to happen is an ongoing priority.

The second of the two common threads through all centers is a focus on vigilantly protecting against infringements of citizens' privacy, civil liberties, and civil rights. Fusion centers are part of a much larger domestic protection enterprise whose mission is safeguarding the American people - including our ability to exercise Constitutional rights and be free from unwarranted government intrusions in our lives. Privacy protections are not an afterthought for the NFCA, the National Network, or our Federal, state, and local partners. In fact, the first order of business last year during the development process of our national strategy was to address privacy, civil liberties, and civil rights. That is why it is literally Goal Number 1 in the strategy: "Uphold public confidence through the safeguarding of information and the protection of the person and the privacy, civil rights, and civil liberties of individuals." We cannot achieve our collective mission without the public's trust and confidence.

All fusion centers have strong publicly available privacy policies in place, we train our people on them, and we emphasize transparency. Privacy policies have been established across all 50 States and all operational fusion centers at least as comprehensive as the Information Sharing Environment (ISE) Privacy Guidelines. Training has occurred for more than 200,000 local, tribal, state, and federal front line officers to identify and report suspicious activity in accord with the ISE Suspicious Activity Reporting (SAR) Functional Standard, and several thousand analysts have been trained in accord with vetting guidelines to ensure that ISE SARs are demonstrably behavior-based and their handling (retention, redress, and other related considerations) is fully compliant with privacy policies. The very first initiative in our strategy relates to training and education for law enforcement and public safety partners on fusion centers' role in the protection of privacy, civil rights, and civil liberties. The strategy's second initiative relates to conducting assessments on the impact of certain technologies on privacy, civil liberties, and civil rights of citizens, and developing policies to mitigate any impact *prior* to procurement. We look to the Technology Policy Framework published by the IACP in January of 2014 to support these efforts.

Counterterrorism analysis and information sharing functions are components of the fusion center mission but they are not - and they should not be - the sole components. That is because our fusion centers report to governors, state law enforcement executives, county, and municipal public safety leadership. They do not report to the Federal government, nor should they. The vast majority of fusion centers including ours in Montana are "all-crimes" centers, which reflects the fact that criminal intelligence analysis, data sources, interagency relationships, and information sharing capabilities resident in the centers are useful for all types of investigations - not just terrorism. While the Federal interest in fusion centers relates primarily to their ability to contribute to

counterterrorism efforts, the reality is that the fusion process is effective for any public safety effort. Case in point is the discussion we are having today - certain transnational organized criminal groups may not be linked to terrorism, but those groups pose an even more direct threat - and impact - to American citizens every day. Whether the crime is terrorism, child abduction, gang violence, drug trafficking, or oil field theft, the fusion process maximizes efforts to prevent, deter, or investigate the crime. Institutionalized collaboration through information sharing and co-location is effective no matter the nature of the crime. Our Federal partners benefit from the all-crimes approach because it amounts to “drilling” on real-world scenarios using the fusion center critical operational capabilities every day. When a terrorism threat emerges, fusion center participants and customers “know the drill.”

We are still often asked about the difference between fusion centers and JTTFs. To be clear: 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 then 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 -- the Torrance, California gas station robberies, the smuggling of cigarettes in North Carolina, the sale of pseudoephedrine in California -- actually is linked to terrorist activity.

It does not make sense to try to separate crime and terror in our daily work of analyzing threat information and criminal activity. We have to knock that wall down. If we're going to continue to improve, we have to understand that the sharing of information makes communities safer. Our ultimate goal is to prevent terrorism. But in every community across the country there are violent crimes that terrorize neighborhoods and families and affect lives and businesses every day. Fusion centers are uniquely situated to do things that JTTFs or no other program can do. We can bring together disparate resources, data sets, analytical perspectives, and personnel in order to analyze and share information on terror, crime, or other threats to public safety. We can make sure that JTTFs get the information they need from state and local partners, but that the DEA and CBP and HSI and chiefs and sheriffs and governors get the information they need about non-terrorism public safety threats as well.

National Strategy for the National Network of Fusion Centers, 2014-2017

In July of 2013, the House Homeland Security Committee released a report titled “Majority Staff Report on the National Network of Fusion Centers.” It reflected the painstaking work of several committee staff who visited more than 30 fusion centers across the country and met with dozens of federal, state, and local fusion center partners. The findings of this report contrasted significantly with a 2012 report from this committee’s Permanent Subcommittee on Investigations that was highly critical of fusion centers. Among the key findings of the House committee’s 2013 report was an acknowledgement that “the National Network is a National asset that needs to realize its full potential to help secure the Homeland.” The report also recognized the direct impact of fusion center information sharing on terrorism investigations by noting that according to information provided by the FBI and DOJ, between December 2008 and December 2012, “176 SARs [suspicious activity reports] entered by fusion centers into the eGuardian or Shared Spaces SAR databases [...] resulted in the FBI opening new terrorism investigations.” “Additionally, 289 Terrorist Watchlist encounters reported by fusion centers enhanced existing FBI cases.” The level of productivity mentioned in the 2013 House report has increased since it was published. In the one-year period between August 2013 and July 2014, 238 SARs submitted by fusion centers supported FBI investigations. When I hear people question the value of fusion centers to federal counterterrorism efforts, I point them directly to these statistics. The value of fusion centers to homeland security efforts is clear.

In late 2013 the NFCA formed a working group comprised of law enforcement and other public safety groups, emergency management, and the National Governors Association, and dedicated hundreds of hours to developing a strategy to shape the continued maturation of the National Network of Fusion Centers. The resulting work - the National Strategy for the National Network of Fusion Centers 2014-2017 - was published in July of 2014. The strategy can be found at our website: www.nfcausa.org.

The strategy objectives and priority initiatives are now driving efforts to improve analysis and sharing around all types of threats, and this will lead to enhanced collaboration in addressing border-related transnational organized criminal threats. It is an ambitious strategy - we specified 37 initiatives that advance each of the strategy’s four goals. The strategy development process was just the beginning. While several initiatives are already well underway, we are in process of developing an implementation plan that to prioritize our actions through 2017 to achieve objectives under the strategy. In addition to our national strategy, we worked with DHS Intelligence & Analysis, the FBI, and other members of the Information Sharing and Access Interagency Policy Committee (ISA-IPC - the federal interagency forum that oversees the planning and implementation of the Information Sharing Environment) to support their development of

a Federal “Engagement Strategy” which is fully complementary with our strategy. Working together with our Federal partners, we identified a dozen initiatives that will be joint priorities over the next several years. For the first time, there is a clear Federal strategy that directly supports the state and locally driven National Network.

Central to that support is our ongoing engagement with the DHS Office of Intelligence and Analysis. The National Network continually relies on our partners at I&A. The support provided by I&A personnel assigned to fusion centers is critically important. I&A Undersecretary General Frank Taylor and his staff have invested considerable time and effort in determining the best path forward for I&A’s deployment of personnel in the field. They have regularly interacted with the NFCA and sought our input along with that of our state and local partners. Unfortunately, the Intelligence Authorization Act of 2014 constrained I&A’s choices through limiting language in the classified annex to the bill - a move that was made by the Intelligence Committees without consulting any fusion center directors or other state and local stakeholders impacted by the decision.

The impact of the new I&A field deployment plan won’t be known until the changes are in place, but there is concern across the National Network about what it will mean for fusion center connectivity to certain classified systems and information that is essential to sharing threat intelligence with state and local law enforcement and other public safety partners. One of the primary objectives in the fusion center strategy is enhancing analytical collaboration in the field. Limiting I&A presence in fusion centers threatens to inhibit that collaboration, including with regard to border-related transnational criminal threats.

As NFCA President Mike Sena testified on the House side last month, every fusion center should have an I&A intelligence professional with the authority to collect and share raw information to include release authority, execute joint production, and effectively share information across all classification levels. Decisions regarding the appropriate type of intelligence professional for each fusion center should be the result of discussions between those state and regional fusion centers and I&A.

In addition to the assignment of personnel, DHS provides important training opportunities for analysts in fusion centers. In particular, DHS facilitates the delivery of specialized analytic seminars focused on specific threat topic areas such as gangs, drugs, and borders for fusion center analysts. The seminars bring together a diverse range of state and local subject-matter experts (SMEs) and partner agencies/organizations from all levels of government to inform analytic efforts. These seminars provide a welcome opportunity for fusion center and federal analysts to discuss emerging threats, trends, and patterns and collaborate on joint products and best practices. Montana has benefited from attending these seminars both as a trainee and a SME.

Technology Policy Challenges Impacting Law Enforcement's Ability to Share Information to Detect, Prevent, and Investigate Threats

To *share* information we have to *have* it in the first place, as well as mechanisms to *communicate* it across the public safety enterprise. Tips and leads - "see something say something" - from members of the public, police officers, sheriffs' deputies, and Federal agents are one very important source of such information. In the 21st Century, technology applications are increasingly important sources of valuable information. Just as the private sector in America is continually adopting new methods of generating useful information and communicating with one another via new technologies, American law enforcement and public safety at all levels must adopt the latest technological innovations in order to adapt to increasingly sophisticated criminals - especially criminal organizations and terrorist organizations that are operating and communicating across national borders with much more freedom than ever before.

The use of technology by law enforcement and intelligence agencies also comes with important limitations, restrictions, checks, and balances that the private sector does not have to deal with. That slows down our ability to adopt technology and tap its full potential, but we understand why. We in law enforcement fully appreciate that these restrictions are rooted in the Constitution that grants all of us our sacred freedoms. We abide by the laws, policies, and regulations that help to give the public confidence that its government is respecting privacy, civil rights, and civil liberties as it carries out its mission of protecting people and finding perpetrators when crimes are committed.

We get concerned, however, when policies threaten to completely eliminate or render minimally useful our adoption of new technology or access to data. We have a responsibility to share our informed perspectives with policymakers to help understand the implications of policy decisions on our ability to investigate crimes or generate intelligence that can help prevent crime or terrorism. The thing we fear is knowing - in the aftermath of a deadly event - that we could have had access to information to prevent or identify a threat ahead of time, but a law or policy prevented our timely access to it. We currently adhere to all the requirements of 28 CFR Part 23 regarding data retention and other issues, and we are used to taking measures like these. We expect it. But we believe it is important to understand the implications of adding new restrictions without fully considering the implications on our ability to share information.

Today we are dealing with several of these types of issues: the "going dark" challenge that renders warrants for communications intercepts useless; device encryption issues that prevent the gathering of either incriminating or exculpatory evidence after a crime has occurred; automated license plate recognition (ALPR) technology provides

investigative leads with anonymous data, but is being severely restricted in some areas with short data retention policy mandates and is even prohibited in other areas. Policy decisions on these and other issues will have an impact on our ability to generate and share information to detect, prevent, and investigate crime and terrorism - including along our national borders.

Technology is also how we enable fast, efficient sharing of information across jurisdictions. In Montana and across the National Network of Fusion Centers we have embraced technology to assist us in the gathering, analysis and dissemination of information. After the critical shooting incidents in Newtown, Connecticut, the Aurora Theater and the Sikh Temple in Wisconsin, to name just a few examples, fusion centers worked to enhance our ability to share timely and accurate information across the entire the National Network in a real-time environment. Working with Homeland Security Information Network (HSIN) staff at DHS, the Situational Awareness Room or “SitAware” was developed. This communications resource is now utilized routinely by the network and other public safety partners during planned and critical events. It has been used to coordinate information sharing among the National Network and our partners in such events as the Boston bombings, the Super Bowl, and national elections. More recently the SitAware concept has been replicated by the National Network to facilitate better real-time information sharing regarding cyber threats. The Cyber Information Network Awareness Room or “CINAware” has been established through HSIN to assist in responding to emerging cyber threats. Neither of these important efforts could have been possible without the support of DHS. We must continue to support the development and enhancement of technology to improve the availability, dissemination, and coordination of information to fusion centers and our partners.

Conclusion

Chairman Johnson and Ranking Member Carper, thank you on behalf of the Montana Department of Justice and the Montana fusion center for inviting me to testify today. My colleagues in fusion centers across the country are happy to be a resource for you and your staff as you consider how to continue effectively supporting strong collaboration among those of us who protect our fellow citizens.