Statement for

Committee on Emerging Threats and Spending Oversight

United States Senate Committee on Homeland Security & Governmental Affairs

"Lessons Learned: 10 Years Since the Boston Marathon Bombings"

Kerry Sleeper

Special Advisor, Secure Community Network

26 April 2023

Chairperson Hassan, Ranking Member Romney, other distinguished members of the Committee, it is my privilege to appear before you today in my current role as Senior Advisor for the Secure Community Network, the official safety and security organization for the Jewish community in North America.

I would also like to acknowledge my fellow panelist, Ed Davis, the former Commissioner of the Boston Police Department, and Rich Serino, the former Deputy Administrator of the Federal Emergency Management Agency, both of whom played integral leadership roles in both preparing for and responding to the Boston Marathon bombing on April 15, 2013.

My testimony regarding "Lessons Learned: "10 Years Since the Boston Marathon Bombings" will be focused on intelligence and information sharing efforts; those initiatives intended to prevent or mitigate acts of targeted violence.

In the years after 9/11 and preceding the Boston Marathon bombing, the domestic intelligence architecture, or the process of how federal, state, and local law enforcement shared threat information, underwent a remarkable enhancement and transformation. It was understood that state and local law enforcement played a pivotal role in protecting their communities from acts of targeted violence. It followed that the federal government needed to ensure they integrated their intelligence efforts with their state and local partners. From this understanding grew critical information sharing processes such as the FBI's Joint Terrorism Task Forces, state and local Fusion Centers, and DHS's See Something Say Something® campaign, also known as Suspicious Activity Reporting.

With these processes in place, state and local fusion centers could receive sensitive or classified threat information from their federal partners, analyze or assess that

information for context in the communities they serve, develop intelligence products to share within their community to convey the threat, and encourage Suspicious Activity Reporting information back for further investigation or analysis efforts. In addition, the FBI's Joint Terrorism Task Forces, or JTTFs, numbering over 200 across the nation with hundreds of state and local officers assigned, were developed to investigate both international and domestic threats of terrorism.

Both the Boston Regional Intelligence Center – the city of Boston's fusion center – and the Boston Field Office JTTF played critical roles in supporting intelligence and information sharing requirements in the security planning for the Boston Marathon, as well as the investigative phase and apprehension of the perpetrators.

One of the most important lessons learned in the intelligence and information sharing efforts was that Tamerlan Tsarnaev had been the subject of an FBI assessment prior to the bombing. The assessment alleged he appeared to be radicalizing with potential ties to a foreign terrorist organization, although the assessment was eventually closed for lack of additional information.

The information on this assessment of Tsarnaev was not provided to state and local law enforcement, and the logical question was asked, if they had known, could they have disrupted the plotting? More precisely, could state and local law enforcement have pursued the allegation of Tsarnaev's radicalization beyond what the FBI Domestic Investigations and Operations Guide (DIOG) legally allowed?

This question, and lesson learned, resulted in a swift change in JTTF protocols for state and local JTTF members. The FBI clarified that the names of individuals who were the subject of assessments or threats were to be shared with the relevant law enforcement agencies and/or state and local JTTF members. This action, or lesson

learned, impacted state and local law enforcement agencies by providing transparency into the subjects of JTTF investigations across the country.

The positive lesson learned from the Marathon bombing is when great leaders exemplify and drive the importance of collaboration, the public is well protected. Both Rich and Ed, seated in front of you, emulate that spirit of collaboration.

Now, I would like to discuss the gaps I see in security for today's threat environment, specifically in the area of intelligence and information sharing to prevent mass casualty attacks.

As devastating as the Boston bombing was to both Boston and our Nation, we are in a far more complex and dynamic threat environment then we were in 2013.

Individuals with little or aspirational association to terror or hate groups, citing personal grievances or affiliation to a cause, calling for death and destruction, are committing mass casualty attacks at a record pace. Whether the intent is terroristic, criminal, or due to an underlying mental health issue, the deadly results are the same to the victims and the communities where they occur, as well as our society more broadly. Public gatherings, special events, parades, schools, places of worship, grocery stores, retail businesses, funeral homes, and street corners are all recent locations of these tragedies.

The causation of this rise in deadly targeted violence is complex, but it can be more successfully understood and mitigated with a more effective whole of government approach to intelligence and analysis of the threats and the individuals committing these acts of violence. Unfortunately, since COVID, we have seen a significant degrading in our national collaboration between federal, state and local law enforcement. In short, the system is breaking down. People and agencies are not talking to each other. This deficiency has been widely observed by law

enforcement leadership across the county and recently documented in the 2022 Intelligence Summit Post-Event Report, a convening hosted by the Department of Homeland Security and the International Association of Chiefs of Police, in coordination with law enforcement, intelligence, and homeland security partners across the nation.

Since 2004, the preeminent process for federal, state and local law enforcement to coordinate their intelligence and information sharing efforts in meeting emerging threats was the Criminal Intelligence Coordinating Council (CICC). The CICC serves as the voice for all levels of law enforcement on the best use of criminal intelligence to keep the country safe.

The CICC has successfully provided interagency law enforcement coordination on critical issues, to include fusion centers, suspicious activity reporting, coordination with JTTFs, and how to manage emerging threats on a national level. The CICC, under the Global Advisory Committee, serves as a Federal Advisory Committee and advises the U. S. Attorney General. The oversight of the CICC currently resides within the Bureau of Justice Assistance (BJA). BJA urgently needs additional resources to reinvigorate the CICC for the specific intent of bringing together federal, state and local law enforcement leadership, with appropriate private sector participation, to strategize on how best to meet today's complex and dynamic threat environment. Without this convening process, efforts to mitigate our evolving threat environment will be left to local authorities and ad hoc efforts.

I don't need to inform this body that law enforcement resources across our nation are facing critical shortages, swatting incidents across our country are further stretching those resources in feigned calls of active shooters at schools, medical facilities, and workplaces. Given the high number of actual recent mass shootings, authorities have no option but to respond with all available resources.

Foreign and domestic terrorism, mass shootings, hate crimes, threats on social media, deep and dark web usage by offenders, are all inextricably intertwined and highlight both the dynamic nature and complexity of today's threat environment. Those threats we face require the development of a national strategy that integrates EVERY law enforcement agency into the plan and solution. That plan requires an understanding of the threat through detailed analysis, up-to-date tools and technology to access the threat, updated training to utilize the tools and adapt to the constantly evolving nature of the threat, and the rapid sharing of threat information to prevent an attack once there is evidence of a likely attack. There needs to be a central focal point for this type of planning and collaboration, but to date, that is not occurring at the national level to the degree we require. The strengthening of the CICC would be a significant step forward you could undertake to ensure the type of collaboration required to meet today's threat environment is taking place.