Department of Justice

STATEMENT OF

MICHAEL B. STEINBACH
ASSISTANT DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

COMMITTEE ON HOMELAND SECURITY
U.S. HOUSE OF REPRESENTATIVES

AT A HEARING ENTITLED

"TERRORISM GONE VIRAL:
THE ATTACK IN GARLAND, TEXAS AND BEYOND"

PRESENTED

JUNE 3, 2015

Statement of
Michael B. Steinbach
Assistant Director
Federal Bureau of Investigation

Before the
Committee on Homeland Security
U.S. House of Representatives

At a Hearing Entitled
"Terrorism Gone Viral: The Attack in Garland, Texas and Beyond"

Presented
June 3, 2015

Good morning Chairman McCaul, Ranking Member Thompson, and Members of the committee. Thank you for the opportunity to appear before you today to discuss the widespread reach of terrorists' influence, which transcends geographic boundaries like never before. As technology advances so, too, does terrorists' use of technology to communicate – both to inspire and recruit. The widespread use of technology propagates the persistent terrorist message to attack US interests whether in the Homeland or abroad. As the threat to harm Western interests evolves, we must adapt and confront the challenges, relying heavily on the strength of our federal, state, local, and international partnerships.

We continue to identify individuals who seek to join the ranks of foreign fighters traveling in support of the Islamic State of Iraq and the Levant, commonly known as ISIL, and also homegrown violent extremists who may aspire to attack the United States from within. These threats remain among the highest priorities for the FBI and the Intelligence Community as a whole.

Conflicts in Syria and Iraq continue to serve as the most attractive overseas theaters for Western-based extremists who want to engage in violence. We estimate upwards of 200 Americans have traveled or attempted to travel to Syria to participate in the conflict. While this number is lower in comparison to many of our international partners, we closely analyze and assess the influence groups like ISIL have on individuals located in the United States who are inspired to commit acts of violence. Whether or not the individuals are affiliated with a foreign terrorist organization and are willing to travel abroad to fight or are inspired by the call to arms to act in their communities, they potentially pose a significant threat to the safety of the United States and U.S. persons.

ISIL has proven relentless in its violent campaign to rule and has aggressively promoted its hateful message, attracting like-minded extremists to include Westerners. To an even greater degree than al-Qa'ida or other foreign terrorist organizations, ISIL has persistently used the internet to communicate. From a Homeland perspective, it is ISIL's widespread reach through the internet and social media which is most concerning as ISIL has aggressively employed this technology for its nefarious strategy. ISIL blends traditional media platforms, glossy photos, in-depth articles, and social media campaigns that can go viral in a matter of seconds. No matter the format, the message of radicalization spreads faster than we imagined just a few years ago.

Unlike other groups, ISIL has constructed a narrative that touches on all facets of life – from career opportunities, to family life, to a sense of community. The message isn't tailored solely to those who are overtly expressing symptoms of radicalization. It is seen by many who

click through the internet every day, receive social media push notifications, and participate in social networks. Ultimately, many of these individuals are seeking a sense of belonging.

As a communication medium, social media is a critical tool for terror groups to exploit. One recent example occurred last week. An individual was arrested for providing material support to ISIL by facilitating an associate's travel to Syria to join ISIL. The arrested individual had multiple connections, via a social media networking site, with other like-minded individuals.

As I've stated in previous opportunities I've had to testify before this committee, there is no set profile for the susceptible consumer of this propaganda. However, one trend continues to rise – the inspired youth. We've seen certain children and young adults drawing deeper into the ISIL narrative. These individuals are often comfortable with virtual communication platforms, specifically social media networks.

ISIL continues to disseminate their terrorist message to all social media users – regardless of age. Following other groups, ISIL has advocated for lone wolf attacks. In recent months ISIL released a video, via social media, reiterating the group's encouragement of lone offender attacks in Western countries, specifically advocating for attacks against soldiers and law enforcement, intelligence community members, and government personnel. Several incidents have occurred in the United States and Europe over the last few months that indicate this "call to arms" has resonated among ISIL supporters and sympathizers.

In one case, a Kansas-based male was arrested in April after he systematically carried out steps to attack a U.S. military institution and a local police station. The individual, who was

inspired by ISIL propaganda, expressed his support for ISIL online and took steps to carry out acts encouraged in the ISIL call to arms.

The targeting of U.S. military personnel is also evident with the release of hundreds of names of individuals serving in the U.S. military by ISIL supporters. The names were posted to the internet and quickly spread through social media, depicting ISIL's capability to produce viral messaging. Threats to U.S. military and coalition forces continue today.

Across the world, recent events commemorating ANZAC Day, a significant milestone in Australian and New Zealand military history, attracted unwanted attention that could have resulted in violence had Australian authorities not disrupted the plotting efforts underway. These arrests re-emphasize our need to remain vigilant in the Homeland against these small scale attacks.

We should also understand community and world events – as viewed through the eyes of a committed individual – may trigger action. As we've seen with recent highly publicized events, including the attack in Garland, Texas, these acts of terror will attract international media attention and may inspire "copy cat" attacks. The targeting of the Muhammad Art Exhibit and Contest exemplifies the call to arms approach encouraged by ISIL along with the power of viral messaging. In this instance, the event gained much publicity prior to it occurring and attracted negative attention that reached areas of the country – and the world – that it may not have without the widespread reach of the internet. The extensive network coupled with the magnetic messaging provides inspiration and validation that others share their outrage.

Lastly, social media has allowed groups, such as ISIL, to use the internet to spot and assess potential recruits. With the widespread horizontal distribution of social media, terrorists can identify vulnerable individuals of all ages in the United States – spot, assess, recruit and radicalize – either to travel or to conduct a Homeland attack. The foreign terrorist now has direct access into the United States like never before.

In recent arrests, a group of individuals was contacted by a known ISIL supporter who had already successfully traveled to Syria and encouraged them to do the same.

Some of these conversations occur in publicly accessed social networking sites, but others take place via private messaging platforms. As a result, it is imperative the FBI and all law enforcement organizations understand the latest communication tools and are positioned to identify and prevent terror attacks in the Homeland. We live in a technologically driven society and just as private industry has adapted to modern forms of communication so too have the terrorists. Unfortunately, changing forms of internet communication are quickly outpacing laws and technology designed to allow for the lawful intercept of communication content. This real and growing gap the FBI refers to as "Going Dark" is the source of continuing focus for the FBI, it must be urgently addressed as the risks associated with "Going Dark" are grave both in traditional criminal matters as well as in national security matters. We are striving to ensure appropriate, lawful collection remains available. Whereas traditional voice telephone companies are required by CALEA to develop and maintain capabilities to intercept communications when law enforcement has lawful authority, that requirement does not extend to most Internet communications services. As a result, such services are developed and deployed without any

ability for law enforcement to collect information critical to criminal and national security investigations and prosecutions.

The FBI, in partnership with the Department of Homeland Security, is utilizing all lawful investigative techniques and methods to combat the threat these individuals may pose to the United States. In conjunction with our domestic and foreign partners, we are rigorously collecting and analyzing intelligence information as it pertains to the ongoing threat posed by foreign terrorist organizations and homegrown violent extremists. In partnership with our many federal, state, and local agencies assigned to Joint Terrorism Task Forces around the country, we remain vigilant to ensure the safety of the American public. Be assured, the FBI continues to pursue increased efficiencies and information sharing processes as well as pursue technological and other methods to help stay ahead of threats to the Homeland.

Chairman McCaul, Ranking Member Thompson, and Committee Members, I thank you for the opportunity to testify concerning terrorists' use of the internet and social media as a platform for spreading ISIL propaganda and inspiring individuals to target the Homeland. I am happy to answer any questions you might have.