Department of Justice

STATEMENT OF
MICHAEL STEINBACH
EXECUTIVE ASSISTANT DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE
COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
UNITED STATES SENATE

AT A HEARING CONCERNING
THE FEDERAL GOVERNMENT'S EFFORTS TO MONITOR, DISRUPT, AND COUNTER TERRORIST PROPAGANDA, WITH PARTICULAR FOCUS ON THE ISLAMIC STATE OF IRAQ AND THE LEVANT'S ("ISIL") ONLINE COMMUNICATIONS

PRESENTED
JULY 6, 2016

STATEMENT OF
MICHAEL STEINBACH
EXECUTIVE ASSISTANT DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE
COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
UNITED STATES SENATE

AT A HEARING CONCERNING
THE FEDERAL GOVERNMENT'S EFFORTS TO MONITOR, DISRUPT, AND COUNTER TERRORIST PROPAGANDA, WITH PARTICULAR FOCUS ON THE ISLAMIC STATE OF IRAQ AND THE LEVANT'S ("ISIL") ONLINE COMMUNICATIONS

PRESENTED
JULY 6, 2016

Good afternoon Chairman Portman, Ranking Member McCaskill, and Members of the Subcommittee. 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. Their widespread use of technology propagates the persistent terrorist message to attack U.S. interests whether in the Homeland or abroad. As these threats to Western interests evolves, we must adapt and confront the challenges, relying heavily on the strength of our Federal, State, local, and international partnerships.

Preventing terrorist attacks remains the FBI's top priority. The terrorist threat against the United States remains persistent and acute. The threats posed by foreign fighters, including those recruited from the U.S., traveling to join the Islamic State of Iraq and the Levant ("ISIL") and from homegrown violent extremists are extremely dynamic.

ISIL has proven relentless in its violent campaign to rule and has aggressively promoted its hateful message, attracting like-minded extremists, including among Westerners. To an even greater degree than al Qaeda or other foreign terrorist organizations, ISIL has persistently used the Internet to communicate and spread its message. From a Homeland perspective, it is ISIL's widespread reach through the Internet and particularly 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 is not 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.

As a communication medium, social media is a critical tool that terror groups can 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 have testified previously, there is no set profile for the susceptible consumer of this propaganda. However, one trend continues to rise — the inspired youth. We have 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. Ultimately, many of these individuals are seeking a sense of belonging.

ISIL continues to disseminate its terrorist message to all social media users — regardless of age. Following other groups, ISIL has advocated for attacks by lone individuals. Several incidents have occurred in the United States and Europe over the last year that indicate this "call to arms" has resonated among ISIL supporters and sympathizers.

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, demonstrating ISIL's capability to produce viral messaging. Threats to U.S. military and coalition forces continue today.

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

Some of these conversations occur in publicly accessed social networking sites, but others take place via private messaging platforms. 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 lawful access to communication content. This growing gap the FBI refers to as Going Dark is the source of continuing focus for the FBI; it must be urgently addressed as there are grave risks for both 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. Although law enforcement may access stored communications with lawful process, some services are being developed that do not store communications, and, therefore, do not givelaw enforcement the ability 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 Portman, Ranking Member McCaskill, and subcommittee 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.