Mark F. Giuliano
Deputy Director, Federal Bureau of Investigation
Statement for the Record
The Washington Institute for Near East Policy
Wednesday, May 28, 2014

1. Introduction

Good afternoon. Thank you to everyone with The Washington Institute for Near East Policy for hosting me today. I am pleased to be able to join you to provide you with an overview of how we are adapting and evolving, the current counterterrorism threat, and the challenges the United States and its partners are facing as a result of the conflict in Syria.

I previously spoke here three years ago in April 2011 when I was Assistant Director for our Counterterrorism Division, and I am honored to be invited back in my new role as Deputy Director.

First, in order to address the threats we are facing it is critical to have the resources we need. Coming in, Director Comey knew the budget would be one of his top priorities, and he was vocal with Congress and with the public about the nature of the FBI's work, as well as the importance of having the resources to get the job done.

Fortunately, the FBI was allocated $8.3 billion in FY 2014, our largest allocation to date, so that we can carry out our mission. The last few fiscal years prior we were cutting programs, so this is a welcome change. As the Director has said, we are grateful to have the budget that we do, and we need to be faithful stewards of that money. It will be spent with the goal of ensuring that the FBI is prepared to face the multitude of ever-evolving threats our nation faces.

The FBI's mission to protect the American people has never been broader – and the demands upon the Bureau have never been greater – but Director Comey has a strong vision of where the Bureau needs to go down the road. When he first became Director, he

was surprised to learn how far the FBI had come in its transition to a full partner in the Intelligence Community. And that's a fair assessment. Most people aren't aware of all the changes we've made in the past 12 years, nor do they understand the breadth and scope of our capabilities. Our job is to prevent attacks, and those stories rarely make the headlines.

2. Adapting and Evolving to Stay Ahead of the Threat

Before I comment on the current counterterrorism threat and the crisis in Syria, I wanted to address how the FBI is adapting and evolving to stay ahead of the threat.

As the U.S. Government's lead domestic intelligence agency, the FBI is a threat-focused, intelligence-driven organization *now*, but there is still work to be done. We are committed to always looking ahead into the future to see how we need to adapt to stay *ahead* of the threat.

As such, the Bureau is pushing for the full integration of intelligence in operations across the board – not just in counterterrorism – while respecting the rule of law and the safeguards guaranteed by the Constitution.

We've made great strides in prioritizing our threats through our Threat Review and Prioritization Process, but we are perpetually seeking to become even more threat-driven.

Our Threat Review and Prioritization Process, or TRP, helps the Bureau develop a standard national picture of our threats, and to streamline the prioritization process for both the Field and FBI Headquarters. Additionally, it provides the Field with clear guidance and a consistent process to evaluate threats, while ensuring Headquarters has an effective way to program manage and evaluate the significant threats facing the country.

Another way we are integrating intelligence into operations is through our Fusion Cell Model which integrates our intelligence and operational elements through teams of analysts embedded with Special Agents in operational divisions. These analysts evaluate both national and international information and provide intelligence on current and

emerging threats across programs – making connections that are not always visible at the Field level.

The TRP and the Fusion Cell Model, among other resources we are employing, help us to be more aware of emerging threats and to stop them before they can occur.

The full integration of intelligence into operations will remain a strong priority for the Director. It is only by fully maturing this process that we will be able to effectively address the terrorist threat.

Finally, we are also addressing and staying ahead of the threat by working with our state, local, federal, and international partners. Whether it is through our Joint Terrorism Task Forces (JTTFs), Field Intelligence Groups, the Fusion Centers, or any other FBI task force, we know that to succeed we cannot address the threats we face alone.

3. Cyber

I would be remiss if I didn't also make a few comments on cyber. It has become one of the greatest threats to our national security, and some aspect of cyber – whether it be cyber crime, the targeting of U.S. national security assets, critical infrastructure, the economy, or foreign hostile intelligence operations conducted over the Internet – is involved in many of the cases and threats we are working.

We are confronting cyber threats in a number of ways, and we are re-tooling to address the threat, just as we did in the counterterrorism arena after September 11, 2001.

To address this threat, there have been sweeping changes across the FBI's Cyber program through the Next Generation Cyber initiative. These changes have not been limited to one division, but rather have had an impact across the FBI.

The FBI's strategy to address increasing cyber threats has proven quite successful in gaining unprecedented visibility into the problem, and in coordinating operational responses. This strategy includes leveraging the FBI-led National Cyber Investigative Joint Task Forces (NCIJTF) – the focal point for the coordination and integration of

counterintelligence, counterterrorism, intelligence, and law enforcement activities of more than 18 member agencies in order to identify and disrupt cyber threats.

We are also working closely with our federal, state, and local partners on cyber task forces in all 56 field offices and with our 64 legal attaches' offices around the world. We are focused on targeting high-level intrusions, the biggest and most dangerous botnets, state-sponsored attacks, and global cyber rings.

Additionally, we are coordinating and working closely with our private sector partners utilizing iGuardian to instill confidence that we can protect their proprietary and customer data. We have to think *strategically* – be better, smarter, and to do so quickly. iGuardian is a secure information portal allowing industry-based, individual partners to report cyber intrusion incidents in real-time. The iGuardian portal is an evolution of eGuardian, the platform through which the FBI's law enforcement partners provide potential terrorism-related threats and suspicious activity reports. While eGuardian enlists law enforcement users, iGuardian was developed specifically for partners within critical telecommunications, defense, banking and finance, and energy infrastructure sectors and is available over the sensitive but unclassified InfraGard network.

While challenges remain, we are making great strides. On May 19, 2014, FBI New York announced a number of law enforcement actions related to the investigation and takedown of the company Blackshades. Blackshades had been selling and distributing malicious software to thousands of individuals throughout the world. Blackshades' flagship product – a Remote Access Tool – was a sophisticated piece of malware that enabled its users to remotely and surreptitiously gain complete and total control over a victim's computer.

Once installed, the user of the tool could access and view documents, photographs, record keystrokes, and even activate the web camera on the victim's computer – all without the victim's knowledge. We believe that the tool was purchased by thousands of people around the world and used to infect more than 700,000 computers in more than 100 countries. The FBI New York Cyber Division's outreach efforts and strong relationships with private sector and international partners were critical to the success in this case.

Another recent success was against five members of the People's Liberation Army of China (PLA). These officers, members of the 3PLA, used a variety of techniques, including malicious emails that appeared to be from individuals familiar to the targets, to install backdoors to penetrate the network security of six companies. Once gaining access they ultimately stole proprietary information related to trade secrets, financial information, production capabilities, and business strategies, among other company assets. Economic espionage is a genuine threat that U.S. companies are facing, and this first indictment of Chinese cyber actors clears the way for additional charges to be made in the future. The FBI, in coordination with the Department of Justice, will continue to use every tool at our disposal to fight cyber espionage to protect U.S. innovation, ideas, and our competitive advantage in the world marketplace.

The cyber threat cannot be stopped by just those individuals working in one division of one organization – it is a U.S. Government problem that we have to work on together – with the interagency, with our friends in the private sector, and especially with our partners overseas. This is a threat which is likely to continue to evolve and will remain a top FBI priority for years to come.

4. Counterterrorism Threat

With regard to counterterrorism, the threats we face, in terms of both understanding and getting in front of them, have never been more complex.

In 2013, the JTTFs successfully disrupted more than 100 counterterrorism threats. While core al Qa'ida has been degraded, our counterterrorism efforts are challenged by a combination of the decentralization of the violent extremist movement, shifting alliances of like-minded violent extremist organizations, and the general instability in the Middle East and North Africa.

The threat has become more flat, and by that I mean increasingly more complex and decentralized. Terrorists aren't just operating in the shadows – they target English-speaking audiences, and actively use the Internet, social media, and propaganda like al

Qa'ida in the Arabian Peninsula's, or AQAP's, *Inspire Magazine* to recruit and provide guidance on how to attack our critical infrastructure and economy.

Our enemies are sophisticated in their use of the Internet and all forms of electronic communications, which has provided them with a much easier means of acquiring information and exercising command and control over their operations – from recruiting to planning to propaganda to execution.

While al Qa'ida central is not the dominant force it was 12 years ago, it remains intent on causing as much death and destruction as possible. A more serious threat, I believe, stems from al Qa'ida affiliates such as AQAP and the Islamic State of Iraq and the Levant (ISIL), which was formerly known as al Qa'ida in Iraq (AQI).

AQAP in particular attempted several attacks on the United States, including the failed Christmas Day airline bombing in 2009, and the attempted bombing of U.S.-bound cargo planes in October 2010.

As the Boston Marathon bombings illustrate, we also face a continuing threat from homegrown violent extremists. These individuals present unique challenges because they do not share a typical profile and may be self-radicalized, self-trained, and self-executing. Their experiences and motives are often distinct, but they are increasingly savvy and willing to act alone, which makes them difficult to identify and to stop.

In the past three years, we have seen homegrown extremists attempt to detonate bombs at high profile targets, such as the Federal Reserve Bank in New York, commercial establishments in downtown Chicago, the Pentagon, and the U.S. Capitol. Fortunately, these attempts – and many others – were prevented, but the threat remains real.

As the lead agency responsible for countering terrorist threats to the United States and its interests overseas, the FBI integrates intelligence and operations to detect and disrupt terrorists.

We have the capacity to collect information, review it, and push out intelligence products to the rest of the IC to aid in our collective national security efforts, and we are a leader in many areas of expertise, technical collection, cyber, and national security.

In order to succeed in this environment – an environment which is constantly changing, ever-evolving, and increasingly more complex – we must be nimble, adept, and able to change quickly. Most importantly, we must work with our partners closely to identify future threats so that we are able to get *ahead* of them.

5. Foreign Fighters in Syria

We are also closely monitoring the unrest in Syria. This crisis is a concern not only for the U.S. Government, but for our overseas partners as well.

As Director Comey recently discussed with the *Wall Street Journal*, the Syrian civil war poses a growing, long-term security threat and is a similar situation to when fighters were traveling to Afghanistan in the 1980s and 1990s. These individuals formed al Qa'ida and declared war on the United States.

With its porous borders, Syria (since about March 2011) has attracted thousands of individuals from across the world interested in participating in the conflict, either in support of Sunni extremist opposition groups or pro-Asad regime elements. Given the global impact of the Syrian conflict, the FBI regularly engages with fellow U.S. Government agencies, the Intelligence Community, and our foreign counterparts in an effort to pursue increased information sharing with our partners on identified foreign fighters, combating radicalization, and exchanges regarding community outreach programs and policing strategies. Through this collaboration, the FBI is working hard to ensure foreign fighters from other nations do not enter the United States undetected. The FBI has also expanded its team within our Counterterrorism Division to fully track, analyze, and ultimately neutralize the threats emanating from Syria to the United States.

Given the prolonged nature of the Syrian conflict the FBI remains concerned that U.S. persons will continue to be attracted to the region and may attempt to travel to Syria to participate in the conflict.

This concern is predominantly centered on:

- The potential contact travelers could have with extremist elements;
- Battlefield experiences they could obtain; and
- The possibility they could become radicalized, or further radicalized, and then conduct organized or lone-wolf style attacks (particularly if they return to their countries of origin).

The recent flood of militants into the country poses a serious challenge as these individuals could be trained to plan and carry out attacks around the world. It is also possible that foreign terrorist organizations could seek to leverage U.S. or Western persons to facilitate terrorist activity, as al-Qa'ida and its affiliates continue to adjust their tactics, techniques, and procedures for targeting the West.

Several U.S. persons have been identified after traveling, or attempting to travel, to participate in the conflict in Syria. Since March 2013, the FBI has arrested a few individuals who either fought in Syria and returned to the United States, or attempted to travel to join in the conflict either with Syrian opposition groups or pro-Asad regime elements.

A few examples of this include Eric Harroun, Basit Javed Sheikh, and Mohammad Hassan Hamdan:

- In March 2013, the FBI arrested Arizona-based Eric Harroun upon his return to the United States from Turkey after having fought in Syria with al-Nusrah Front;
- North Carolina-based Basit Javed Sheikh was arrested in November 2013 for attempting to provide material support to al-Nusrah Front as he was attempting to board a flight overseas to join al-Nusrah Front.
- In March 2014, Michigan-based Mohammad Hassan Hamdan was arrested at the Detroit Metropolitan Airport as he was attempting to travel to Syria to fight alongside Hizballah, a foreign terrorist organization.

The key take-away for us is that this conflict has resulted in a real long-term threat for the United States and its interests. There is not only potential for further radicalization, but the cross-over and collaboration of various terrorist groups.

6. Conclusion

To succeed in combating terrorism we must remain intelligence-driven, continue to scan for looming threats, *effectively* share information with the right people at the right time, and continue our close collaboration with our partners around the world; the U.S. Intelligence Community; federal, state, local, and tribal law enforcement; and public and private organizations. Close relationships with our partners is a requisite for the success of the FBI's unique national security and law enforcement missions. We must do all of this while respecting the rule of law and safeguards guaranteed by the Constitution.

The American public expects much from us, as they should. They deserve excellence, and they expect us to be a team. And they are right. We must be a team to be successful.

Thank you again for having me here today. I'm happy to take your questions.