July 14, 2016

Worldwide Threats to the Homeland: ISIS and the New Wave of Terror

Committee on Homeland Security, United States House of Representatives, One Hundred Fourteenth Congress, Second Session

---

HEARING CONTENTS:

Member Statements

Witnesses

Available Webcast(s)*:

[Watch Full Webcast]

** Please Note: External links included in this compilation were functional at the time of its creation but are not maintained thereafter.*

Compiled From*:

https://homeland.house.gov/hearing/worldwide-threats-homeland-isis-new-wave-terror-2/

** Please Note: External links included in this compilation were functional at the time of its creation but are not maintained thereafter.*

Statement of Chairman Michael McCaul (R-TX)
Homeland Security Committee

Worldwide Threats to the Homeland: ISIS and the New Wave of Terror
July 14, 2016

Remarks as Prepared

Before I begin today's hearing I would like to take a moment to remember the Dallas police officers who lost their lives in the line of duty last week. We will never forget.

The tragedy reminds us that every day our first responders take risks to protect us, and we can honor their sacrifice by showing that we support them and that we have their backs.

The past month we witnessed four major terrorist attacks, in four weeks, in four countries, including the deadliest terrorist attack on the U.S. homeland since 9/11.

All of these attacks are believed to be the work of ISIS, the new standard-bearer of evil. In fact, the group has now been linked to almost 100 plots against the West since 2014—an unprecedented wave of terror.

Nearly 15 years after 9/11, we must confront the reality that we are not winning the war against Islamist terror.

While groups like ISIS may be losing some ground in Syria and Iraq, overall they are not "on the run," as the Obama Administration says. They are on the rise.

But I am concerned that we have only seen the tip of the iceberg.

Director Comey, you prophetically warned this Committee two years ago that there would eventually be a "terrorist diaspora" out of Syria and Iraq, with jihadists returning home to spread extremism.

The exodus has now begun. Thousands of Western foreign fighters have departed the conflict zone, including operatives who are being sent to conduct attacks, as we saw in Paris and Brussels. At the same time, ISIS' online recruiting has evolved, and they now micro-target followers by language and country.

Although our nation is shielded by two oceans, geography alone cannot protect us from this mortal threat.

The statistics speak for themselves. In the past two years, federal authorities have arrested more than 90 ISIS supporters here in our country, and in 2015 we saw more homegrown jihadist plots than we have ever tracked in a single year.

I commend your agencies for stopping dozens of potential tragedies, but too many have already slipped through the cracks. And we know that more plots are in the pipeline.

In the wake of Orlando, Americans are demanding to know how we got to this point, and a clear majority of them say Washington is not doing enough to roll back the threat.

They are stunned by the political correctness here in our nation's capital, especially the refusal to call the threat what it is. We must define the threat in order to defeat it—just as we did with communism and fascism.

We cannot hide the truth, and we cannot redact it from reality. So let's be frank about the enemy: we are fighting radical Islamists.

These fanatics have perverted a major religion into a license to kill and brutalize. And while their beliefs do not represent the views of a majority of Muslims, they represent a dangerous global movement bent on conquering and subjugating others under their oppressive rule.

Sadly, we have failed to commit the resources needed to win. I was recently on the USS Truman aircraft carrier in the Persian Gulf, where our sailors are launching sorties to destroy ISIS positions. While I am proud of their efforts, I am not encouraged by our progress.

Last month, even CIA Director John Brennan gave the Administration a failing grade in the fight and said that, quote, "our efforts have not reduced the group's terrorism capability and global reach."

The President is sticking to a "drip, drip" strategy that is better suited for losing a war than winning one. And each day we stick with half-measures, ISIS is able to dig in further and advance a murderous agenda across the globe. Another day to plot, another day to kill.

The violence is becoming so frequent that we now simply refer to jihadist attacks by the name of the city in which they were perpetrated: Paris. Chattanooga. San Bernardino. Brussels. Orlando. Istanbul.

How many more will be added to the list before we get serious about taking the fight to the enemy?

This is the greatest threat of our time, and I urge each of you today to explain to this Committee—and to the American people—how you are planning to elevate our defenses to keep Americans safe.

###

Prepared Testimony

Secretary of Homeland Security Jeh Charles Johnson
House Committee on Homeland Security

July 14, 2016

Chairman McCaul, Representative Thompson, and members of the Committee, thank you for holding this annual threats hearing with me, the FBI Director and the Director of NCTC. I believe this annual opportunity for Congress to hear from us, concerning threats to the homeland is important. I welcome the opportunity to be here again.

Counterterrorism

San Bernardino and Orlando are terrible reminders of the new threats we face to the homeland.

We have moved from a world of terrorist-directed attacks, to a world that also includes the threat of terrorist-inspired attacks – attacks by those who live among us in the homeland and self-radicalize, inspired by terrorist propaganda on the internet. By their nature, terrorist-inspired attacks are often difficult to detect by our intelligence and law enforcement communities, could occur with little or no notice, and in general, make for a more complex homeland security challenge.

This threat environment has required a whole new type of response.

As directed by President Obama, our government, along with our coalition partners, continues to take the fight militarily to terrorist organizations overseas. ISIL is the terrorist organization most prominent on the world stage. Since September 2014, air strikes and special operations have in fact led to the death of a number of ISIL's leaders and those focused on plotting external attacks in the West. At the same time, ISIL has lost about 47% of the populated areas it once controlled in Iraq, and thousands of square miles of territory it once controlled in Syria. But as ISIL loses territory, it has increased its plotting on targets outside of Iraq and Syria, and continues to encourage attacks in the United States.

On the law enforcement side, the FBI continues to, in my judgment, do an excellent job of detecting, investigating, preventing, and prosecuting terrorist plots here in the homeland.

Following the attacks in Ottawa, Canada in 2014, and in reaction to terrorist groups' public calls for attacks on government installations in the western world, I

directed the Federal Protective Service to enhance its presence and security at various U.S. government buildings around the country.

The Department of Homeland Security has intensified our work with state and local law enforcement, and strengthened our information sharing efforts. Almost every day, we share intelligence and information with Joint Terrorism Task Forces, fusion centers, local police chiefs and sheriffs. And we are now able to instantly cross-reference suspects against law enforcement and counterterrorism databases and share information—often in almost real-time—with our domestic as well as international partners. We are also enhancing information sharing with organizations that represent businesses, college and professional sports, community and faith-based organizations, and critical infrastructure.

And, since 2013 we've spearheaded something called the "DHS Data Framework" initiative. We are improving our ability to use DHS information for our homeland security purposes, and to strengthen our ability to compare DHS data with other travel, immigration, and other information at the unclassified and classified level. We are doing this consistent with laws and policies that protect privacy and civil liberties.

We also provide grant assistance to state and local governments around the country, for things such as active shooter training exercises, overtime for police officers and firefighters, salaries for emergency managers, emergency vehicles, and communications and surveillance equipment. We helped to fund an active shooter training exercise that took place in the New York City subways last November, a series of these exercises earlier this year in Miami and Louisville, and just last month at Fenway Park in Boston. In February, and last month, we announced another two rounds of awards for FY 2016 that will fund similar activities over the next three years.

We are enhancing measures to detect and prevent travel to this country by foreign terrorist fighters.

We are strengthening the security of our Visa Waiver Program, which permits travelers from 38 different countries to come to the U.S. for a limited time period without a visa. In 2014, we began to collect more personal information in the Electronic System for Travel Authorization, or "ESTA" system, that travelers from Visa Waiver countries are required to use. ESTA information is screened against the same counterterrorism and law enforcement databases that travelers with traditional visas are screened, and must be approved prior to an individual boarding a plane to the United States. As a result of these enhancements, over 3,000 additional travelers were denied travel here through this program in FY 2015. In August 2015, we introduced further security enhancements to the Visa Waiver Program.

Through the passage in December of the Visa Waiver Program Improvement and Terrorist Travel Prevention Act of 2015, Congress has codified into law several of these security enhancements, and placed new restrictions on eligibility for travel to the U.S. without a visa. We began to enforce these restrictions on January 21, 2016. Waivers from these restrictions will only be granted on a case-by-case basis, when it is in the law enforcement or national security interests of the United States to do so. Those denied entry under the Visa Waiver Program as a result of the new law may still apply for a visa to travel to the U.S. In February, under the authority given me by the new law, I also added three countries – Libya, Yemen and Somalia – to a list that prohibits anyone who has visited these nations in the past five years from traveling to the U.S. without a visa. In April, DHS began enforcing the mandatory use of high security electronic passports for all Visa Waiver Program travelers. In both February and June, CBP enhanced the ESTA application with additional questions.

We are expanding the Department's use of social media for various purposes. Today social media is used for over 30 different operational and investigative purposes within DHS. Beginning in 2014 we launched four pilot programs that involved consulting the social media of applicants for certain immigration benefits. USCIS now also reviews the social media of Syrian refugee applicants referred for enhanced vetting, and is extending this review to additional categories of refugee applicants. Based upon the recommendation of a Social Media Task Force within DHS, I have determined, consistent with relevant privacy and other laws, that we must expand the use of social media even further.

CBP is deploying personnel at various airports abroad, to pre-clear air travelers before they get on flights to the United States. At present, we have this pre-clearance capability at 15 airports overseas. And, last year, through pre-clearance, we denied boarding to over 10,700 travelers (or 29 per day) before they even got to the United States. As I said here last year, we want to build more of these. In May 2015, I announced 10 additional airports in nine countries that we've prioritized for preclearance. In May, CBP announced an "open season," running through August 1, for foreign airports to express interest in participating in the next round of preclearance expansion. I urge Congress to pass legislation enabling preclearance operations in Canada, by providing legal clarity to CBP officials who are responsible for the day-to-day operation of preclearance facilities there.

For years Congress and others have urged us to develop a system for biometric exit – that is, to take the fingerprints or other biometric data of those who leave the country. CBP has begun testing technologies that can be deployed for this nationwide. With the passage of the FY 2016 Omnibus Appropriations Act, Congress authorized up to $1 billion in fee increases over a period of ten years to help pay for the implementation of biometric exit. In April, the Department delivered its Comprehensive Biometric Entry/Exit Plan to Congress, which details CBP's plan for expanding implementation of a

biometric entry/exit system using that funding. I have directed that CBP redouble its efforts to achieve a biometric entry/exit system, and to begin implementing biometric exit, starting at the highest volume airports, in 2018.

Last January I announced the schedule for the final two phases of implementation of the REAL ID Act, which go into effect in January 2018 and then October 2020. At present, 24 states are compliant with the law, 28 have extensions, and 4 states or territories are out of compliance without an extension. Now that the final timetable for implementation of the law is in place, we urge all states, for the good of their residents, to start issuing REAL ID- compliant drivers' licenses as soon as possible.

In the current threat environment, there is a role for the public too. "If You See Something, Say Something"™ must be more than a slogan. We continue to stress this. DHS has now established partnerships with the NFL, Major League Baseball and NASCAR, to raise public awareness at sporting events. An informed and vigilant public contributes to national security.

In December we reformed "NTAS," the National Terrorism Advisory System. In 2011, we replaced the color-coded alerts with NTAS. But, the problem with NTAS was we never used it, it consisted of just two types of Alerts: "Elevated" and "Imminent," and depended on the presence of a known specific and credible threat. This does not work in the current environment, which includes the threat of homegrown, self-radicalized, terrorist-inspired attacks. So, in December we added a new form of advisory – the NTAS "Bulletin" – to augment the existing Alerts, and issued the first Bulletin providing the public with information on the current threat environment and how they can help. The December Bulletin expired last month, and we issued a new and updated Bulletin on June 15.

Given the nature of the evolving terrorist threat, building bridges to diverse communities is also a homeland security imperative. Well informed families and communities are the best defense against terrorist ideologies. Al Qaeda and ISIL are targeting Muslim communities in this country. We must respond. In my view, building bridges to our communities is as important as any of our other homeland security missions.

In 2015 we took these efforts to new levels. We created the DHS Office for Community Partnerships (OCP), which is now the central hub for the Department's efforts to counter violent extremism in this country, and the lead for a new interagency Countering Violent Extremism (CVE) Task Force that includes DHS, the Department of Justice (DOJ), the FBI, the National Counter Terrorism Center (NCTC) and other agencies. We are focused on partnering with and empowering communities by providing them a wide range of resources to use in preventing violent extremist recruitment and radicalization. Specifically, we are providing access to federal grant opportunities for

state and local leaders, and partnering with the private sector to find innovative, community-based approaches.

Ensuring that the Nation's CVE efforts are sufficiently resourced has been an integral part of our overall efforts. Last week, on July 6, I announced the CVE Grant Program, with $10 million in available funds provided by Congress in the 2016 Omnibus Appropriations Act. The CVE Grant Program will be administered jointly by OCP and FEMA. This is the first time federal funding at this level will be provided, on a competitive basis, specifically to support local CVE efforts. The funding will be competitively awarded to state, tribal, and local governments, nonprofit organizations, and institutions of higher education to support new and existing community-based efforts to counter violent extremist recruitment and radicalization to violence.

Finally, given the nature of the current threat from homegrown violent extremists, homeland security must include sensible gun control laws. We cannot have the former without the latter. Consistent with the Second Amendment, and the right of responsible gun owners to possess firearms, we must make it harder for a terrorist to acquire a gun in this country. The events of San Bernardino and Orlando make this painfully clear.

Aviation Security

As we have seen from recent attacks in Egypt, Somalia, Brussels, and Istanbul, the threat to aviation is real. We are taking aggressive steps to improve aviation and airport security. In the face of increased travel volume, we will not compromise aviation security to reduce wait times at Transportation Security Administration (TSA) screening points. With the support of Congress we are surging resources and adding personnel to address the increased volume of travelers.

Since 2014 we have enhanced security at overseas last-point-of-departure airports, and a number of foreign governments have replicated those enhancements. Security at these last-point-of-departure airports remains a point of focus in light of recent attacks, including those in Brussels and Istanbul.

As you know, in May of last year a classified DHS Inspector General's test of certain TSA screening at eight airports, reflecting a dismal fail rate, was leaked to the press. I directed a 10-point plan to fix the problems identified by the IG. Under the new leadership of Admiral Pete Neffenger over the last year, TSA has aggressively implemented this plan. This has included retraining the entire Transportation Security Officers (TSO) workforce, increased use of random explosive trace detectors, testing and re-evaluating the screening equipment that was the subject of the IG's test, a rewrite of the standard operating procedures manual, increased manual screening, and less randomized inclusion in Pre-Check lanes. These measures were implemented on or ahead of schedule.

We are also focused on airport security. In April of last year TSA issued guidelines to domestic airports to reduce access to secure areas, to require that all airport and airline personnel pass through TSA screening if they intend to board a flight, to conduct more frequent physical screening of airport and airline personnel, and to conduct more frequent criminal background checks of airport and airline personnel. Since then employee access points have been reduced, and random screening of personnel within secure areas has increased four-fold. We are continuing these efforts in 2016. In February, TSA issued guidelines to further enhance the screening of aviation workers in the secure area of airports, and in May, TSA and airport operators completed detailed vulnerability assessments and mitigation plans for nearly 300 federalized airports.

We will continue to take appropriate precautionary measures, both seen and unseen, to respond to evolving aviation security threats and protect the traveling public.

Without short-cutting aviation security, we are also working aggressively to improve efficiency and minimize wait times at airport security check points in the face of increased air travel volumes. I thank Congress for approving our two reprogramming requests that have enabled us to expedite the hiring of over 1,300 new TSOs, pay additional overtime to the existing TSO workforce, and convert over 2,700 TSOs from part-time to full-time.

We have also brought on and moved canine teams to assist in the screening of passengers at checkpoints, solicited over 150 volunteers from among the TSO workforce to accept temporary reassignment from less busy to busier airports, deployed optimization teams to the Nation's 20 busiest airports to improve operations, and stood up an Incident Command Center at TSA headquarters to monitor checkpoint trends in real time.

We continue to encourage the public to join TSA Pre✓®. The public is responding. While enrollments a year ago were at about 3,500 daily, now enrollments are exceeding 15,000 a day. For 90% of those who are enrolled and utilize TSA Pre✓®, wait times at TSA checkpoints are five minutes or less.

Airlines and airports are also assisting to address wait times. We appreciate that major airlines and airport operators have assigned personnel to certain non-security duties at TSA checkpoints, and are providing support in a number of other ways. Longer term, we are working with airlines and airports to invest in "Innovation lanes" and other technology to transform the screening of carry-on luggage and personal items.

Our efforts are showing results. Nationwide, the wait time for more than 99% of the traveling public is 30 minutes or less, and more than 90% of the traveling public is waiting 15 minutes or less. But we are not taking a victory lap. Over the Fourth of July holiday weekend, TSA screened 10.7 million travelers. June 30 and July 1 were the

highest-volume travel days we have seen since 2007. During this period, however, the average wait time nationwide in standard security lines was less than ten minutes, while those in TSA Pre-check lines waited an average of less than five minutes.

We plan to do more. The summer travel season continues, followed by holiday travel in the fall and winter. We are accelerating the hiring of an additional 600 TSOs before the end of the fiscal year. And we will continue to work with Congress to ensure TSA has the resources it needs in the coming fiscal years.

As I have said many times, we will keep passengers moving, but we will also keep them safe.

Cybersecurity

Along with counterterrorism, cybersecurity remains a cornerstone of our Department's mission. Making tangible improvements to our Nation's cybersecurity is a top priority for President Obama and for me to accomplish before the end of the Administration.

On February 9th, the President announced his "Cybersecurity National Action Plan," which is the culmination of seven years of effort by the Administration. The Plan includes a call for the creation of a Commission on Enhancing National Cybersecurity, additional investments in technology, federal cybersecurity, cyber education, new cyber talent in the federal workforce, and improved cyber incident response.

DHS has a role in almost every aspect of the President's plan.

As reflected in the President's 2017 budget request, we want to expand our cyber response teams from 10 to 48.

We are doubling the number of cybersecurity advisors to in effect make "house calls," to assist private sector organizations with in-person, customized cybersecurity assessments and best practices.

Building on DHS's "Stop. Think. Connect" campaign, we will help promote public awareness on multi-factor authentication.

We will collaborate with Underwriters Laboratory and others to develop a Cybersecurity Assurance Program to test and certify networked devices within the "Internet of Things" -- such as your home alarm system, your refrigerator, or even your pacemaker.

I have also directed my team to focus urgently on improving our abilities to protect the Federal Government and private sector. Over the past year, the National

Cybersecurity Communications Integration Center, or "NCCIC," increased its distribution of information, the number of vulnerability assessments conducted, and the number of incident responses.

I have issued an aggressive timetable for improving federal civilian cybersecurity, principally through two DHS programs:

The first is called EINSTEIN. EINSTEIN 1 and 2 have the ability to detect and monitor cybersecurity threats attempting to access our federal systems, and these protections are now in place across nearly all federal civilian departments and agencies.

EINSTEIN 3A is the newest iteration of the system, and has the ability to automatically block potential cyber intrusions on our federal systems. Thus far E3A has actually blocked over a million potential cyber threats, and we are rapidly expanding this capability. About a year ago, E3A covered only about 20% of our federal civilian networks. In the wake of the malicious cyber intrusion at the Office of Personnel Management, in May of last year I directed our cybersecurity team to make at least some aspects of E3A available to all federal departments and agencies by the end of last year. They met that deadline. Now that the system is available to all civilian agencies, 50% of federal personnel are actually protected, including the Office of Personnel Management, and we are working to get all federal departments and agencies on board by the end of this year.

The second program, called Continuous Diagnostics and Mitigation, or CDM, helps agencies detect and prioritize vulnerabilities inside their networks. In 2015, we provided CDM sensors to 97% of the federal civilian government. Next year, DHS will provide the second phase of CDM to 100% of the federal civilian government.

I have also used my authorities granted by Congress to issue Binding Operational Directives and further drive improved cybersecurity across the federal government. In May 2015, I directed civilian agencies to promptly patch vulnerabilities on their Internet-facing devices. These vulnerabilities are accessible from the Internet, and thus present a significant risk if not quickly addressed. Agencies responded quickly and mitigated all of the vulnerabilities that existed when the directive was issued. Although new vulnerabilities are identified every day, agencies continue to fix these issues with greater urgency then before the directive.

Last month, I issued a second binding operational directive. This directive mandated that agencies participate in DHS-led assessments of their high value assets and implement specific recommendations to secure these important systems from our adversaries. We are working aggressively with the owners of those systems to increase their security.

In September 2015, DHS awarded a grant to the University of Texas at San Antonio to work with industry to identify a common set of best practices for the development of Information Sharing and Analysis Organizations, or "ISAOs." The University of Texas at San Antonio recently released the first draft of these best practices. They will be released in final form later this year after public comment.

Finally, I thank Congress for passing the Cybersecurity Act of 2015. This new law is a huge assist to DHS and our cybersecurity mission. We are in the process of implementing that law now. As required by the law, our NCCIC has built a system to automate the receipt and distribution of cyber threat indicators at real-time speed. We built this in a way that also includes privacy protections.

In March, I announced that this system was operational. At the same time, we issued interim guidelines and procedures, required by this law, providing federal agencies and the private sector with a clear understanding of how to share cyber threat indicators with the NCCIC, and how the NCCIC will share and use that information. We have now issued the final guidelines and procedures consistent with the deadline set by the law.

I appreciate the additional authorities granted to us by Congress to carry out our mission. Today, we face increasing threats from cyber-attacks against infrastructure and I strongly believe that we need an agency focused on cyber security and infrastructure protection.

I have asked Congress to authorize the establishment of a new operational Component within DHS, the Cyber and Infrastructure Protection agency. We have submitted a plan which will streamline and strengthen existing functions within the Department to ensure we are prepared for the growing cyber threat and the potential for large scale or catastrophic physical consequences as a result of an attack. I urge Congress to take action so we are able to ensure DHS is best positioned to execute this vital mission.

Conclusion

I am pleased to provide the Committee with this overview of the progress we are making at DHS on countering threats. You have my commitment to work with each member of this Committee to build on our efforts to protect the American people.

I look forward to your questions.

Hearing before the House Homeland Security Committee
"Worldwide Threats to the Homeland: ISIS and the New Wave of Terror"

July 14, 2016

Nicholas J. Rasmussen
Director
National Counterterrorism Center

Thank you, Chairman McCaul, Ranking Member Thompson, and Members of the Committee. I appreciate this opportunity to discuss the terrorism threats that concern us most. I am pleased to join my colleagues and close partners, Secretary Jeh Johnson from the Department of Homeland Security (DHS), and Director James Comey of the Federal Bureau of Investigation (FBI).

Over the past several years, we have had great success in strengthening our Homeland security and have made progress in reducing external threats emanating from core al-Qa'ida and the self-proclaimed Islamic State of Iraq and the Levant, or ISIL, due to aggressive counterterrorism (CT) action against the groups. Unfortunately, the range of threats we face has become increasingly diverse and geographically expansive, as we saw with ISIL's recent wave of attacks in Bangladesh, Iraq, Saudi Arabia, and Turkey. As these attacks demonstrate, ISIL's strategy is to weaken the resolve of its adversaries and project its influence worldwide through attacks and propaganda, ultimately perpetuating fear.

The continuing appeal of the violent extremist narrative and the adaptive nature of violent extremist groups continue to pose substantial challenges to the efforts of our CT community. In addition to the attacks overseas, we are no doubt reminded by the shooting in Orlando, Florida, last month that homegrown violent extremists, or HVEs, who are inspired by groups such as ISIL remain an unpredictable threat we face in the Homeland. Because HVEs are frequently lone actors, often self-initiating and self-motivating, their threats are harder to detect and, therefore, harder to prevent. But just as the threat evolves, so do we. We are constantly adapting, and we must continue to improve.

Threat Overview

The attack in Orlando underscores the importance of what we are here today to discuss and the critical nature of our vigilance against homegrown violent extremism. While the reasons for the attack in Florida become known and continue to inform how we detect and respond to these types of incidents, we remain committed to keeping our Nation safe. The best way to combat terrorism is a whole-of-government approach, where federal, state, and local intelligence and law enforcement collaborate.

We expect some HVEs will try to replicate the violence and potentially capitalize on the media coverage and attention that attacks like the one in Florida generated. Although we do not see a large number of these types of threats at the moment, we expect to see an increase in threat reporting around the summer holidays and the large public events, celebrations, and gatherings that accompany them. We will continue to track and monitor the threats and share that information with our partners.

In the past few years, the pool of potential HVEs has expanded. As Director Comey has said, the FBI has investigations on around 1,000 potential HVEs across all 50 states. While HVEs have multiple factors driving their mobilization to violence, this increase in caseload tracks with ISIL's rise in prominence and its large-scale media and propaganda efforts to reach and influence populations worldwide. What we have seen over time is that HVEs—either lone actors or small insular groups—continue to gravitate toward simple tactics that do not require advanced skills or outside training. The majority of HVEs will likely continue to select traditional targets, such as military personnel, law enforcement, and other symbols of the US government. Some HVEs—such as the Orlando shooter in June and the San Bernardino shooters in December 2015—may have conducted attacks against personally significant targets. The convergence of violent extremist ideology and personal grievances or perceived affronts likely played a role in motivating these HVEs to attack.

As we approach 15 years since 9/11, the array of terrorist actors around the globe is broader, wider, and deeper than it has been at any time since that day. ISIL's narrative, rooted in unceasing warfare against all enemies, extends beyond the Syria-Iraq battlefield. ISIL has conducted attacks ranging in tactics and targets—the bombing of a Russian airliner in Egypt; the attacks in Paris at restaurants, a sports stadium, and a concert venue; the killing of hostages and Bangladeshi law enforcement officials in a café in Bangladesh; and the bombing of a crowded commercial district in Baghdad—all of which demonstrate how ISIL can capitalize on local affiliates on the ground for attacks. The threat landscape is less predictable and, while the scale of the capabilities currently demonstrated by most of these violent extremist actors does not rise to the level that core al-Qa'ida had on 9/11, it is fair to say that we face more threats originating in more places and involving more individuals than we have at any time in the past 15 years.

As we recently saw at Istanbul's Ataturk Airport and the attack in Belgium in March, terrorists remain focused on attacks against aviation because they recognize the economic damage that may result from even unsuccessful attempts to down aircraft or against airline terminals, as well as the high loss of life and the attention media devotes to these attacks. Worldwide security improvements in the aftermath of the 9/11 attacks have hardened the aviation sector but have not entirely removed the threat. Violent extremist publications continue to promote the desirability of aviation and its infrastructure for attacks and have provided information that could be used to target the air domain.

We have come to view the threat from ISIL as a spectrum, where on one end, individuals are inspired by ISIL's narrative and propaganda, and at the other end, ISIL members are giving operatives direct guidance. Unfortunately it is not always clear; sometimes ISIL members in Iraq and Syria reach out to individuals in the Homeland to enable others to conduct attacks on their behalf. More often than not, we observe a fluid picture where individuals operate somewhere between the two extremes.

ISIL's access to resources—in terms of both manpower and funds—and territorial control in areas of Syria and Iraq are the ingredients that we traditionally look to as being critical to the group's development of an external operations capability, to include their ability to threaten the Homeland. For that reason, shrinking the size of territory controlled by ISIL, and denying the group access to additional manpower in the form of foreign fighters and operatives, remains a top priority, and success in these areas will ultimately be essential to our efforts to prevent the group from operating as a terrorist organization with global reach and impact. And clearly, progress has been made in these areas. But despite this progress, it is our judgment that ISIL's ability to carry out terrorist attacks in Syria, Iraq,

and abroad has not to date been significantly diminished, and the tempo of ISIL-linked terrorist activity is a reminder of the group's continued global reach.

While ISIL's efforts on the ground in Syria and Iraq remain a top priority for the group's leadership, we do not judge that that there is a direct link between the group's current battlefield status in Iraq and Syria and the group's capacity to operate as a terrorist organization with global capabilities. Their external operations capability has been building and entrenching during the past two years, and we do not think battlefield losses alone will be sufficient to degrade completely the group's terrorism capabilities**.** As we have seen, the group has launched attacks in periods in which the group held large swaths of territory as well as during the past few weeks, as the group feels increasing pressure from the counter-ISIL campaign. In addition to their efforts to conduct external attacks from their safe havens in Iraq and Syria, ISIL's capacity to reach sympathizers around the world through its robust social media capability is unprecedented and gives the group access to large numbers of HVEs.

ISIL spokesman Abu Muhammad Adnani's most recent public statement—which encourages ISIL supporters in the US to conduct attacks in their home countries instead of traveling to Iraq and Syria—may suggest that ISIL recognizes the difficulty in sending operatives to the Homeland for an attack. ISIL likely views the US as a harder target than Europe due to Europe's proximity to the conflict. US ports of entry are under far less strain from mass migration, and US law enforcement agencies are not overtaxed by persistent unrest, as some of our counterparts are overseas.

In Europe, we are concerned about ISIL's demonstrated ability to conduct coordinated attacks by deploying operatives from Syria and Iraq and leveraging European jihadist networks. ISIL attacks in Paris in November and Brussels in March revealed several factors that could enable future operations. First, the role of ISIL's cadre of foreign fighters in planning and executing external operations is key. As we know, several of the Paris and Brussels attackers had experience fighting in Syria, including Paris attack coordinator and operative Abdelhamid Abaaoud.

A second factor that has contributed to ISIL's successful attacks in Europe is the flexibility of their operatives. Those serving as facilitators can transition to attackers for different operations. Some of the Brussels attackers supported the Paris attacks by providing explosives and transportation for operatives. This is a dynamic that the US Government must consider in order to effectively aid our European counterparts in identifying and disrupting future attacks. Finally, ISIL's leveraging of criminal, familial, and communal ties contributes to its ability to advance plotting in Europe. Many operatives involved in the attacks in Paris and Brussels share a similar story of getting involved in criminal activities before becoming radicalized to violence.

Similar to the HVE challenge we face, Europe-based individuals have responded to ISIL's violent message and act on the group's behalf. A violent extremist attacked a police officer and his wife last month in France and pledged his allegiance to ISIL amir Abubakr al-Baghdadi during the hostage situation through a live-streaming social media service.

Last year we confirmed that ISIL had successfully sent several operatives—including at least two of the Paris attackers—from Syria to Western Europe by having them blend in with the flow of some 1 million migrants, asylum seekers, and refugees who traveled from Turkey to Greece in 2015. Although ISIL most likely will continue to seek opportunities to infiltrate these Europe-bound flows when it is operationally expedient to do so, the group probably would prefer other options to deploy operatives to

the Homeland because of the relative difficulties to entering the US via the US Refugee Admissions Program. Specifically, applicants have little-to-no control as to whether the UN will refer them for consideration by the US Refugee Admissions Program. Those refugees who are referred to the US Refugee Admissions Program are then subjected to a process for resettlement of refugees administered by the United Nations High Commissioner for Refugees (UNHCR).

To ensure proper scrutiny of refugee applicants referred to the US by the UNHCR, the National Counterterrorism Center (NCTC) has worked extensively with the screening community to deliver a comprehensive, end-to-end refugee vetting system that streamlines operations without compromising safety, removes stovepipes, and increases transparency across the board. This screening is just one part of a comprehensive system of checks—including the participation of the Departments of Homeland Security, State, Defense, and the FBI as well as additional intelligence agencies—that includes extensive in-person overseas interviews, biographic and biometric assessments, and recurrent vetting.

NCTC screening is done in two ways: The first is identity resolution. We utilize automated programs to correlate biographic information of refugee applicants against the Terrorist Identities Datamart Environment, the US Government's central repository of international terrorist information, for potential matches. All of these computer-generated matches are reviewed by analysts trained to resolve identities. We access other Intelligence Community (IC) holdings to then validate those findings.

The second way is our screening against IC holdings. We screen applicant biographic information against the IC holdings to identify any possible matches to raw intelligence reporting and then conduct analysis to determine any nexus to terrorism.

The tremendous efforts we are undertaking to counter the ISIL threat are absolutely warranted, but I want to stress that we still view al-Qa'ida and the various al-Qa'ida affiliates and nodes as a principal counterterrorism priority. For example, while ISIL is driving most terrorist threats against Europe, we know that the pressures we face on the Continent are not limited to ISIL. The attack on the *Charlie Hebdo* magazine office in Paris by individuals linked to AQAP in January 2015 is a key example of the broad violent extremist threat facing Europe. We would not tier our priorities in such a way that downgrades al-Qa'ida in favor of a greater focus on ISIL. When we are looking at the terrorism threats that we face as a nation, including to the Homeland, al-Qa'ida still figures prominently in that analysis.

We are particularly concerned about al-Qa'ida's safe haven in Syria because we know al-Qa'ida is trying to strengthen its global networks by relocating some of its remaining leadership cadre from South Asia to Syria. These leaders include some who have been part of the group since before the September 11 attacks and, once in Syria, we believe they will work with the al-Qa'ida affiliate there—the Nusrah Front—to threaten the US and our allies.

The Nusrah Front is al-Qa'ida's largest affiliate and one of the most capable armed groups operating in Syria. Its integration of al-Qa'ida veterans provides the group with strategic guidance and enhances its standing within the al-Qa'ida global movement. In April, the US military successfully targeted some of the Nusrah Front's senior members, including long-time al-Qa'ida member and former spokesman for the group in Syria, Abu Firas al-Suri. We will remain vigilant in our efforts to counter this group and the threats it poses to the West.

We believe we have constrained the group's effectiveness and their ability to recruit, train, and deploy operatives from their safe haven in South Asia; however, this does not mean that the threat from core al-Qa'ida in the tribal areas of Pakistan or in eastern Afghanistan has been eliminated. We assess that al-Qa'ida and its adherents in the region still aspire to conduct attacks and, so long as the group can potentially regenerate capability to threaten the Homeland with large-scale attacks, al-Qa'ida will remain a threat. Al-Qa'ida's allies in South Asia—particularly the Haqqani Taliban Network—also continue to present a high threat to our regional interests.

The IC is cognizant to the level of risk the US may face over time if al-Qa'ida regenerates, finds renewed safe haven, or restores lost capability. We are very much on alert for signs that al-Qa'ida's capability to attack the West from South Asia is being restored and would warn immediately if we find trends in that direction. I am confident that the US Government will retain sufficient capability to continue to put pressure on that core al-Qa'ida network and therefore reduce the risk of a resurgence by al-Qa'ida in the region.

We also see increasing competition between violent extremist actors within South Asia itself, between and among the Taliban, ISIL's branch in South Asia, and al-Qa'ida. This is an additional dynamic that we are working to understand. While conflict among terrorist groups may well distract them from their core mission of plotting attacks against Western targets, conflict also serves to introduce a degree of uncertainty into the terrorism landscape that raises questions that I don't think we have answers to yet. This is something we are watching very closely.

Stepping back, there are two trends in the contemporary threat environment that concern us most. First is the increasing ability of terrorist actors to communicate with each other outside our reach with the use of encrypted communications. As a result, collecting precise intelligence on terrorist intentions and the status of particular terrorist plots is increasingly difficult.

There are several reasons for this: exposure of intelligence collection techniques, disclosures of classified information that have given terrorist groups a better understanding of how we collect intelligence, and terrorist groups' innovative and agile use of new means of communicating, including ways that are sometimes beyond our ability to collect, known as "going dark."

Second, while we've seen a decrease in the frequency of large-scale, complex plotting efforts that sometimes span several years, we're instead seeing a proliferation of more rapidly evolving threat or plot vectors that emerge simply by an individual encouraged to take action who then quickly gathers the few resources needed and moves into an operational phase. The so-called "flash-to-bang" ratio—the time between when an individual decides to attack and when the attack occurs—in plotting of this sort is extremely compressed and allows little time for traditional law enforcement and intelligence tools to disrupt or mitigate potential plots.

ISIL is aware of this, and those connected to the group have understood that by motivating actors in their own locations to take action against Western countries and targets, they can be effective, especially if they believe they cannot travel abroad to ISIL-controlled areas. In terms of propaganda and recruitment, ISIL supporters can generate further support for their movement, even without carrying out catastrophic, mass-casualty attacks. And that's an innovation in the terrorist playbook that poses a great challenge.

Countering Violent Extremism (CVE)

The number of individuals going abroad as foreign terrorist fighters to Iraq and Syria only emphasizes the importance of prevention. Any hope of enduring security against terrorism or defeating organizations like ISIL rests in our ability to counter the appeal of terrorism and dissuade individuals from joining them in the first place.

To this end, as announced in January 2016, the Countering Violent Extremism Task Force was stood up to organize federal CVE efforts. The CVE Task Force will be led by the Department of Homeland Security for the first two years; afterward, the Department of Justice will assume leadership. It will be staffed by multiple departments and agencies, including the FBI and NCTC. The main objectives of the task force are to coordinate federal support for ongoing and future research, and establish feedback mechanisms to incorporate sound results; synchronize federal government outreach to, and engagement with, CVE stakeholders and provide technical assistance to CVE practitioners; manage and leverage digital technologies to engage, empower, and connect CVE stakeholders; and work with CVE stakeholders to develop intervention programs.

NCTC continues to refine and expand the preventive side of counterterrorism. We have seen a steady proliferation of more proactive and engaged community awareness efforts across the US, with the goal of giving communities the information and tools they need to see violent extremism in their midst and do something about it before it manifests itself. NCTC, in direct collaboration with DHS and the inter-agency team, has led the creation of CVE tools to build community resilience across the country.

NCTC has sent our officers on multiple occasions to meet with the communities in places such as Denver, Sacramento, Buffalo, and Minneapolis to raise awareness among community and law enforcement audiences about the terrorist recruitment threat. Our briefing is now tailored to address the specific issue of foreign fighter recruitment in Syria and Iraq, and we have received a strong demand signal for more such outreach. The Community Resilience Exercise, a tabletop exercise that brings together local law enforcement with community leadership to run through a hypothetical case-study-based scenario featuring a possible violent extremist or foreign fighter, aims to encourage the creation of intervention models at the local level. In the same way that local partners, including law enforcement, schools, social service providers, and communities, have come together to provide alternative pathways and off-ramps for people who might be vulnerable to joining a gang, we are encouraging our local partners to implement similar models for violent extremism. The more resilient the community, the less likely its members are to join a violent extremist group.

Conclusion

Chairman McCaul, Ranking Member Thompson, and members of the Committee, thank you for the opportunity to testify before you this morning. As we are reminded by the events in Florida as well as globally just a couple of weeks ago, the role that NCTC, FBI, and DHS play in combating terrorism, along with this Committee's support, is critically important. I know the collaboration among all the agencies represented here will continue over the months and years to come in order to continue to protect the Homeland.

Thank you all very much, and I look forward to answering your questions.

Department of Justice

STATEMENT OF
JAMES B. COMEY
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE
COMMITTEE ON HOMELAND SECURITY
U.S. HOUSE OF REPRESENTATIVES

AT A HEARING ENTITLED
"WORLDWIDE THREATS TO THE HOMELAND: ISIS AND THE NEW WAVE OF TERROR"

PRESENTED
JULY 14, 2016

STATEMENT OF
JAMES B. COMEY
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE
COMMITTEE ON HOMELAND SECURITY
U.S. HOUSE OF REPRESENTATIVES

AT A HEARING ENTITLED
"WORLDWIDE THREATS TO THE HOMELAND: ISIS AND THE NEW WAVE OF TERROR"

PRESENTED
JULY 14, 2016

Good afternoon Chairman McCaul, Ranking Member Thompson, and members of the committee. Thank you for the opportunity to appear before you today to discuss the current threats to the homeland and our efforts to address new challenges including terrorists' use of technology to both inspire and recruit. The widespread use of technology permits terrorists to propagate the persistent terrorist message to attack U.S. interests whether in the homeland or abroad. As the threat to harm our interests evolves, we must adapt and confront the challenges, relying heavily on the strength of our Federal, State, local, and international partnerships. Our successes depend on interagency cooperation; among those partners with me today are the Department of Homeland Security and the National Counterterrorism Center with whom we work to address current and emerging threats.

Counterterrorism

Preventing terrorist attacks remains the FBI's top priority. The terrorist threat against the United States remains persistent and acute. The threat 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. The tragic event in Orlando last month is a somber reminder of this threat. The FBI is leading a Federal terrorism investigation with the assistance of our State, local, and Federal partners. The ongoing investigation has developed strong indications of radicalization by this killer, but further investigation is needed to determine if this attack was inspired by foreign terrorist organizations. We are spending a tremendous amount of time trying to understand every moment of the killer's path, to understand his motives, and to understand the details of his life. Our work is very challenging: We are looking for needles in a nationwide haystack, but even more challenging, we are also called upon to figure out which pieces of hay might someday become needles. That is hard work and it is the particular challenge of identifying homegrown violent extremists.

These threats remain the highest priority and create the most serious challenges for the FBI, the U.S. Intelligence Community, and our foreign, State, and local partners. ISIL is

relentless and ruthless in its pursuits to terrorize individuals in Syria and Iraq, including Westerners. We continue to identify individuals who seek to join the ranks of foreign fighters traveling in support of ISIL, and also homegrown violent extremists who may aspire to attack the United States from within. In addition, we are confronting an explosion of terrorist propaganda and training available via the Internet and social networking media. Terrorists readily disseminate poisoned propaganda and training materials to attract easily influenced individuals around the world to their cause. They encourage these individuals to travel, but if the individuals cannot travel, the terrorists motivate them to act at home. This is a significant change and transformation from the terrorist threat our nation faced a decade ago.

ISIL's widespread reach through the Internet and social media is most concerning as the group has proven dangerously competent at employing such tools in furtherance of its nefarious strategy. ISIL uses high-quality, traditional media platforms, as well as widespread social media campaigns to propagate its extremist ideology. Recently released propaganda has included various English language publications circulated via social media.

Social media is used as a tool for groups such as ISIL to spot and assess potential recruits. With greater access to social media platforms, terrorists can spot, assess, recruit and radicalize vulnerable persons of all ages in the United States either to travel to engage in terrorist organization activities or to conduct a homeland attack. Such use of the Internet, including social media, in furtherance of terrorism and other crimes must continue to be addressed by all lawful means, while respecting international obligations and commitments regarding human rights (including freedom of expression), the free flow of information, and a free and open Internet.

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, not necessarily with the initial intention to participate in terrorist activities. Echoing other terrorist groups, ISIL has advocated for lone offender attacks in Western countries. Recent ISIL videos and propaganda specifically advocate for attacks against soldiers, law enforcement, and intelligence community personnel in Western countries. Several incidents have occurred in the United States, Canada, and Europe that indicate this "call to arms" has resonated among ISIL supporters and sympathizers. The challenge here is how to defeat ISIS and thwart its use of the Internet for terrorist and other criminal activity while continuing to help the Internet be a force for good that promotes the enjoyment of freedom of expression, association, and peaceful assembly – especially for individuals who are acutely at risk.

Some of these conversations occur openly on social networking sites, but others take place via private messaging platforms that use encryption. Terrorists' exploitation of encrypted platforms presents serious challenges to law enforcement's ability to identify, investigate, and

disrupt terrorist threats. We respect the right of people to engage in private communications, regardless of the medium or technology. Whether it is instant messages, texts, or old-fashioned letters, citizens have the right to communicate with one another in private without unauthorized government surveillance, because the free flow of information is vital to a thriving democracy.

The United States believes that the Internet has been, and will be, a tremendous force for good – it has enabled the promotion and protection of fundamental freedoms. But the Internet's potential is dependent on people's ability and willingness to use it without undue restrictions and fear. Individuals must be able to trust that there will be respect for privacy, access to information, and freedom of expression, and there will be appropriate legal restraints on government action. Without these protections, the Internet risks becoming a mechanism for social control, rather than a place for all to express and exchange ideas, views, and information. The risks posed by terrorism are great, and the need for law enforcement is strong, but we must balance those requirements against the important role played by free expression in helping to address those same challenges.

The benefits of our increasingly digital lives, however, have been accompanied by new obstacles and, accordingly, we are considering how criminals and terrorists might use advances in technology to their advantage. Investigating and prosecuting these offenders is a core responsibility and priority of the Department of Justice. As national security and criminal threats continue to evolve, the Department has worked hard to stay ahead of changing threats and changing technology. The decisions we make over the next several years about the future of the Internet --- including the laws and policies that are put in place to protect freedom of expression while thwarting terrorist and other criminal activities -- will determine whether our children will continue to enjoy an open, interoperable, secure and reliable Internet. And this in turn will greatly affect whether the Internet will continue to yield the remarkable social, economic and political progress that it has to date.

We must ensure both the right of people to engage in private communications as well as the protection of the public. The more we as a society rely on electronic devices to communicate and store information, the more likely it is that information that was once found in filing cabinets, letters, and photo albums will now be stored only in electronic form. When changes in technology hinder law enforcement`s ability to exercise investigative tools and follow critical leads, those changes also hinder efforts to identify and stop terrorists who are using social media to recruit, plan, and execute an attack in our country.

We are seeing more and more cases where we believe significant evidence resides on a phone, a tablet, or a laptop — evidence that may be the difference between an offender being convicted or acquitted. If we cannot access this evidence, it will have ongoing, significant impacts on our ability to identify, stop, and prosecute these offenders.

The FBI is using all lawful investigative techniques and methods to combat these terrorist threats to the United States, including both physical and electronic surveillance. Along with our

domestic and foreign partners, we are collecting and analyzing intelligence about the ongoing threat posed by foreign terrorist organizations and homegrown violent extremists. We continue to encourage information sharing. In partnership with our many Federal, State, local, and tribal agencies assigned to Joint Terrorism Task Forces around the country, we remain vigilant to ensure the safety of the American public. 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.

Intelligence

Integrating intelligence and operations is part of the broader intelligence transformation the FBI has undertaken in the last decade, and while we are making progress, we still have more work to do. Our goal every day is to get better at using, collecting, and sharing intelligence to better understand and defeat our adversaries.

We have established an Intelligence Branch within the FBI to lead integration across the organization, with responsibility for all intelligence strategy, resources, policies, and functions. The branch is headed by an Executive Assistant Director who looks across the entire enterprise and drives integration. We have also established a Bureau Intelligence Council within the Intelligence Branch to ensure we take a consolidated and integrated approach to threats. As part of this council, senior-level intelligence professionals will lead enterprise-wide strategic assessments, facilitate a broader understanding of how threats mitigated across operational programs are related, and help balance our priorities with those of the broader intelligence community and U.S. government.

We have also put in place training for all levels of the workforce, from entry-level employees to senior leaders, to ensure we achieve that integration throughout the enterprise. New agents and analysts now engage in practical training exercises and take core courses together at the FBI Academy — and, as a result, are better prepared to collaborate effectively throughout their careers. In addition, all field supervisory agents, supervisory analysts, and foreign language program managers, as well as headquarters unit chiefs, now attend a two-day forum focused on sharing best practices to advance integration. All section chiefs and GS-15 field agents and analysts also attend a two-and-a-half-day course on effectively integrating intelligence processes to maximize resources against prioritized threats. Finally, our entire executive management team at headquarters has participated in two integration sessions to ensure the integration of intelligence into every aspect of the FBI's work.

In addition, we are dedicated to expanding the developmental and leadership opportunities for all members of the intelligence program workforce. We recently put in place seven additional Senior Supervisory Intelligence Analyst positions in various offices around the country to increase leadership opportunities for our analyst cadre and enhance our management of field intelligence work. These GS-15 analysts manage intelligence in the field, fulfilling a

role that has traditionally been performed by agents and demonstrating we are promoting effective integration throughout the organization.

We have also redesigned the training curriculum for another part of the Intelligence Program workforce — Staff Operations Specialists ("SOSs") — to aid in their performance of tactical functions in the field. In addition, a new development model clearly identifies SOS work responsibilities, tasks, training, and opportunities at the basic, intermediate, and advanced levels to guide the professional growth of SOSs across the organization at all points throughout their FBI careers.

Similarly, our language workforce continues to make important contributions to the mission. Our language professionals have recently supported numerous important investigations and operations, including Malaysia Airlines Flight 17 last summer, numerous ISIL-related investigations, the disruption of a nuclear threat in Moldova, and so many others. The National Virtual Translation Center ("NVTC") also continues to provide excellent service, supporting hundreds of government offices each year.

The FBI cannot be content to just work what is directly in front of us. We must also be able to understand the threats we face at home and abroad and how those threats may be connected. Toward that end, intelligence is gathered, consistent with our authorities, to help us understand and prioritize identified threats and to determine where there are gaps in what we know about these threats. We then seek to fill those gaps and learn as much as we can about the threats we are addressing and others on the threat landscape. We do this for national security and criminal threats, on both a national and local field office level. We then compare the national and local perspectives to organize threats into priorities for each of the FBI's 56 field offices. By categorizing threats in this way, we strive to place the greatest focus on the gravest threats we face. This gives us a better assessment of what the dangers are, what's being done about them, and where we should prioritize our resources.

Cyber

Virtually every national security and criminal threat the FBI faces is cyber-enabled in some way. We face sophisticated cyber threats from foreign intelligence agencies, hackers for hire, organized crime syndicates, and terrorists. These threat actors constantly seek to access and steal classified information, our trade secrets, our technology, and our ideas — things of incredible value to all of us and of great importance to our national and economic security. They seek to strike our critical infrastructure and to harm our economy.

The pervasiveness of the cyber threat is such that the FBI and other intelligence, military, homeland security, and law enforcement agencies across the Federal government view improving cyber security and preventing cyber-attacks as a top priority. Within the FBI, we are targeting the most dangerous malicious cyber activity: high-level intrusions by state-sponsored hackers and global organized crime syndicates, as well as the most prolific botnets. We need to

be able to move from reacting to such malicious activity after the fact to preventing such attacks. That is a significant challenge, but one we embrace.

As the committee is well aware, the frequency and impact of malicious cyber activity on our nation's private sector and government networks have increased dramatically in the past decade and are expected to continue to grow.

We continue to see an increase in the scale and scope of reporting on malicious cyber activity that can be measured by the amount of corporate data stolen or deleted, personally identifiable information compromised, or remediation costs incurred by U.S. victims. For example, as the committee is aware, the Office of Personnel Management ("OPM") discovered last year that a number of its systems were compromised. These systems included those that contain information related to the background investigations of current, former, and prospective Federal government employees, as well as other individuals for whom a Federal background investigation was conducted. The FBI is working with our interagency partners to investigate this matter.

Another growing threat to businesses and individuals alike is ransomware, which is malicious software that takes control of victims' computers and systems and encrypts the data until the victims pay a ransom. Last year alone reported losses from ransomware totaled more than $24 million. The FBI works closely with the private sector so that companies may make informed decisions in response to ransomware and other malware attacks. Companies can prevent and mitigate malware infection by utilizing appropriate back-up and malware detection and prevention systems, and training employees to be skeptical of emails, attachments, and websites they don't recognize. The FBI does not encourage payment of ransom, as payment of extortion monies may encourage continued criminal activity and paying a ransom does not guarantee that an organization will regain access to its data.

The FBI is engaged in a myriad of efforts to combat cyber threats, from efforts focused on threat identification and information sharing inside and outside of government, to our emphasis on developing and retaining new talent and changing the way we operate to defeat these threats. We take all potential threats to public and private sector systems seriously and will continue to investigate and hold accountable those who pose a threat in cyberspace.

Finally, the strength of any organization is its people. The threats we face as a nation have never been greater or more diverse and the expectations placed on the Bureau have never been higher. Our fellow citizens look to us to protect the United States from all of those threats and the men and women of the Bureau continue to meet and exceed those expectations, every day. I want to thank them for their dedication and their service.

Chairman McCaul, Ranking Member Thompson, and committee members, I thank you for the opportunity to testify concerning the threats to the Homeland. I am happy to answer any questions you might have.