SEPTEMBER 10, 2014

CYBERSECURITY, TERRORISM, AND BEYOND:

ADDRESSING EVOLVING THREATS TO THE HOMELAND

U.S. SENATE, COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

ONE HUNDRED THIRTEENTH CONGRESS, SECOND SESSION

HEARING CONTENTS:

OPENING STATEMENTS :

- **Rep. Thomas R. Carper (R-DE)** **[View PDF]**
  Chairman, Committee on Homeland Security and Governmental Affairs

WITNESSES:

- **Honorable Francis X. Taylor** **[View PDF]**
  Under Secretary for Intelligence and Analysis,
  Department of Homeland Security
- **Honorable Suzanne E. Spaulding** **[View PDF]**
  Under Secretary,
  National Protection and Programs Directorate
  Department of Homeland Security
- **Nicholas J. Rasmussen** **[View PDF]**
  Deputy Director,
  National Counterterrorism Center
  Office of the Director of National Intelligence
- **Robert Anderson, Jr.** **[View PDF]**
  Executive Assistant Director,
  Criminal, Cyber, Response, Cyber, Response, and Services Branch,
  Federal Bureau of Investigation
  Department of Justice

AVAILABLE WEBCAST(S):*

- *Full Committee Hearing*

COMPILED FROM:

- *http://www.hsgac.senate.gov/hearings/cybersecurity-terrorism-and-beyond-addressing-evolving-threats-to-the-homeland*

** Please note: Any external links included in this compilation were functional at its creation but are not maintained thereafter.*

Opening Statement of Chairman Thomas R. Carper:
"Cybersecurity, Terrorism, and Beyond:
Addressing Evolving Threats to the Homeland"
September 10, 2014

As prepared for delivery:

Almost every year, this committee holds a hearing to review a multitude of threats to our homeland and examine how our government is working to counter them. We routinely hear from the Department of Homeland Security, the FBI and the National Counter Terrorism Center about how we can best keep Americans safe from those who seek to carry out deadly attacks against our country and its people. We also hear about actors in cyberspace that want to drain our bank accounts, shut down our financial system and our electric grid, steal our individually identifiable information and our identities, as well as the R & D that will enable American businesses and our military to remain pre-eminent in the world.

Assessing these ever-changing, broad threats and making sure our government continues to hone its ability to stop them remains a top priority for this committee, particularly as we approach another 9/11 anniversary. This year, our hearing takes on an added significance, as our nation confronts a growing terrorist threat in Iraq and Syria. As we sit here today, our military is engaging in limited airstrikes in Iraq in an effort to dislodge and repel that threat. Later this evening, President Obama will address our nation. He is expected to share with us and the world the steps that he is recommending be taken in Iraq and in Syria to reverse the expansion of the Islamic State of Iraq and Syria and enable the people who live in those countries to reclaim their lives.

Much of the world has been exposed to a steady stream of deeply disturbing images from that region in recent weeks. Brutal executions. Human rights atrocities. Repression of women. And a seemingly endless procession of masked militants defiantly waiving the black flag of jihad in celebration of their brutality. Effectively addressing the threat from the newly-proclaimed Islamic State of Iraq and Syria will require a multifaceted strategy. That strategy will need a military component and the development of a robust international coalition to execute it. Among the goals of that strategy is to ensure that the Islamic State of Iraq and Syria does not establish a long-term safe haven from which it can launch attacks against either our allies or our homeland – much like we saw with al Qaeda in the days before 9/11.

Today, we will examine the steps that our federal government has already taken, along with the steps we still need to take, to prevent this from happening. We will drill down on this threat and its impact on our homeland, both in this open hearing as well as in a classified briefing directly following. That's not all we're going to do, though. In addition to examining the more conventional terrorist threat the instability in Iraq and Syria may pose, we will also closely examine another major threat that affects our homeland daily: cyber attacks.

Every day, nation states and their affiliates, criminals, terrorists, and hackers launch cyber attacks against our government agencies, our businesses, and important parts of our daily lives such utilities and financial networks. Some of these actors want to steal our sensitive information to sell it on the black market or to gain a competitive edge. Others are trying to make a political point. Some, however, would like to use a cyber attack to cause wide-scale economic damage or even physical harm. Many of them are good at it, and they're getting even better. We need to stay a step ahead of them. Today, we'll hear in the open portion of this hearing and also in the closed portion how we plan to do that, not unlike the steps we've taken to address terror threats in the wake of 9/11.

Congress clearly has a role to play here. Actually, several roles. One of them is an oversight role. It's one that we take very seriously. Another is a legislative role that involves developing legislation to help enable America to anticipate and repel the cyber attacks that we face on an almost 24/7 basis today. In the last several months, this Committee has completed action and reported three separate cyber bills unanimously to the full Senate. One bill would significantly enhance the capabilities of the Department of Homeland Security's cyber workforce. Another would better protect federal agencies from cyber attack. And, a third would codify the cyber center that the Department uses to monitor and respond to attacks to strengthen its ability to do so.

Yesterday, in an op-ed in "The Hill" newspaper, Secretary Johnson recognized the bipartisan efforts of this Committee and talked about the critical need to pass cyber legislation this Congress – I couldn't agree more. In closing, as we mark the anniversary of 9/11 tomorrow, we must keep in mind one of the key lessons we learned since that fateful day thirteen years ago—the threat is always evolving. Not that long ago, crooks used to have to rob a bank to steal our money. Now, they can click a button on a distant computer and accomplish the same goal. Nation states and rival businesses used to employ corporate insiders or retirees to steal company secrets. Now, they send a spear-phishing email. And terrorists used to be a distant threat in the mountains of Afghanistan or Pakistan. Now, an increasing number of them are homegrown. They may be using European, or even, American passports.

So as the threats become more sophisticated, more elusive, and more diffuse, we need to remain ever vigilant to ensure that our government is nimble enough to keep up with tomorrow's threats as they confront us. We have come a long way since 9/11. In many respects, we are more secure than we were on this day thirteen years ago, but the world in which we live remains a dangerous place, so there is always more work to do. When it comes to securing the homeland and anticipating the next threat, we owe it to the American people to strive for perfection. The consequences of failure are simply too high, and the costs too severe.

I'm pleased that we have with us today a panel of witnesses who work together every day to tackle the terrorist and cyber threats we face. Let me express my gratitude to each of you for your testimony and also thank you for your service to our country.

###

Statement for the Record

The Honorable Suzanne E. Spaulding

Under Secretary, National Protection and Programs Directorate

and

The Honorable Francis X. Taylor

Under Secretary, Office of Intelligence and Analysis

U.S. Department of Homeland Security

Before the

U.S Senate Committee on Homeland Security and Governmental Affairs

Regarding

Cybersecurity, Terrorism and Beyond:

Addressing Evolving Threats to the Homeland

September 10, 2014

Introduction

Chairman Carper, Ranking Member Coburn and distinguished members of the committee, thank you for the opportunity to appear before you today to discuss terrorist, cyber and other human-caused threats to the Homeland and the current threat environment on the eve of the anniversary of the September 11, 2001 attacks.

Thirteen years later, we continue to face a dynamic threat environment. Threats to the Homeland are not limited to any one individual, group or ideology and are not defined or contained by borders. They display the increasing determination of individuals to carry out acts of terrorism that have potential to negatively impact the Homeland through loss of life, destruction of critical infrastructure, disruption of technological capabilities or services, or compromise of information security.

In the testimony today, we will highlight some of the threats we face and the risk-informed actions we take that assist government at all levels and owners and operators of critical infrastructure to understand evolving threats, share information on these threats and hazards, and promote best practices, training, and tools in the four priority areas outlined by Secretary Johnson: (1) aviation security, (2) border security, (3) countering violent extremism, and (4) cybersecurity.

Challenges Ahead

It is important to mention a couple items to provide some strategic context before covering specifics. First, the cornerstone of our mission at DHS has always been, and should continue to be, counterterrorism – that is, protecting the nation against terrorist attacks. We must remain vigilant in detecting and preventing terrorist threats that may seek to penetrate the homeland from the land, sea or air. From a security perspective, many of the resources we expend and activities we conduct apply to both countering terrorism, as well as countering transnational criminal organizations, and other homeland security challenges.

Second, to address the range of challenges the nation faces most collaboratively and effectively within the Department, we have recently undertaken an initiative entitled "Strengthening Departmental Unity of Effort." In his April 22, 2014 memorandum, Secretary Johnson directed a series of actions to enhance the cohesiveness of the Department, while preserving the professionalism, skill, and dedication of the people within, and the rich history of, the DHS components.

The actions in this initiative: new senior leader forums led by Secretary and the Deputy, and cross-departmental strategy, requirements, and budget development and acquisition processes that are tied to strategic guidance and informed by joint operational plans and joint operations are building and maturing DHS into one that is greater than the sum of its parts – one that operates

much more collaboratively, leverages shared strengths, realizes shared efficiencies, and allows us to further improve our important role as an effective domestic and international partner.

Terrorism and Aviation Security

Core Al Qa'ida, Al-Qa'ida in the Arabian Peninsula (AQAP), and their affiliates remain a major concern for DHS. Despite senior leadership deaths, the group maintains the intent and capability to conduct attacks against U.S. citizens and our facilities, and has demonstrated an ability to adjust its tactics, techniques and procedures for targeting the West in innovative ways. AQAP's three attempted attacks against the U.S. homeland—the airliner plot of December 2009, an attempted attack against U.S.-bound cargo planes in October 2010, and an airliner plot in May 2012— demonstrate their efforts to adapt to security procedures. Over the past several weeks DHS has taken a number of steps to enhance aviation security at overseas airports with direct flights to the United States, and other nations have followed with similar enhancements.

The Islamic State of Iraq and the Levant (ISIL) is a terrorist group operating as if it were a military organization, attempting to govern territory, and their experience and successes on the battlefields of Iraq and Syria have armed them with capabilities most terrorist groups do not possess. The group aspires to overthrow governments in the region and eventually beyond. At present, DHS is unaware of any specific, credible threat to the U.S. Homeland from ISIL. However, violent extremists who support them have demonstrated the intent and capability to target American citizens overseas, and ISIL constitutes an active and serious threat within the region and could attempt attacks on U.S. targets overseas with little-to-no warning. Attacks could also be conducted by supporters acting independently of ISIL direction with little-to-no warning. In January, ISIL's leader publically threatened "direct confrontation" with the United States, which is consistent with the group's media releases during the past several years that have alluded to attacking the United States.

ISIL exhibits a very sophisticated propaganda capability, disseminating high-quality media content on multiple online platforms, including social media, to enhance its appeal. ISIL's English-language messaging and its online supporters have employed—and will almost certainly continue—Twitter "hashtag" campaigns that have gained mainstream media attention and have been able to quickly reach a global audience and encourage acts of violence. Media accounts of the conflict, and propaganda in particular, play a role in inspiring U.S. citizens to travel to Syria. We are aware of a number of U.S. persons who have attempted travel to Syria this year, which underscores their continued interest in partaking in the conflict. More than 100 U.S. persons and over two thousand Westerners have traveled or attempted travel to Syria to participate in the conflict—with some of them seeking to fight with or otherwise support violent extremist groups.

We remain concerned about the threat of U.S. foreign fighters and supporters returning from Syria and whether they would to conduct attacks either on their own initiative or at the direction

of terrorist groups abroad. In addition, a small number of U.S. persons have died while fighting in Syria—including the first suicide bombing by an identified U.S. person in Syria in May and at least one other recently killed while fighting alongside ISIL. These foreign fighters, many in possession of Western passports, have likely become further radicalized while receiving additional training and experience, and pose a potential threat upon their return to their home countries.

The DHS Office of Intelligence and Analysis (I&A) is working closely with interagency partners to evaluate threat data and ensure relevant information reaches DHS personnel and state, local, tribal and territorial (SLTT) partners who can use this information to reduce risks to the Homeland. For example, I&A, the Federal Bureau of Investigation (FBI), and the National Counterterrorism Center, produced a poster, handout and muster language for DHS screeners to have background about the conflict in Syria. To ensure our SLTT and private sector partners are kept informed of the current ISIL threat, I&A has hosted multiple calls with our partners in recent months to examine the ongoing situation and, jointly with the FBI, released Joint Intelligence Bulletins (JIB) that provided context and background, examined the potential retaliatory threat and ISIL's use of social media to publicize the group's actions and goals. Following the 9/11 attacks, the importance of an informed community of first responders became clear. I&A places priority on ensuring that the Nation's first responders have the information that they need to identify the trends, tactics and behaviors of a terrorist. It also takes a vigilant public; the Department is dedicated to reminding Americans that "If You See Something, Say Something."

Border Security

Border security must include an intelligence-driven, risk-based approach that focuses resources on the places where our surveillance and intelligence tells us the threats to border security exist, and prepares us to move when the threat moves. The collaborative intelligence work of I&A, the U.S. Coast Guard, the U.S. Customs and Border Protection and the U.S. Immigration and Customs Enforcement helps keep our Southern and Northern borders safe each and every day. We ensure that the officers that are protecting the border points of entry are informed of the necessary intelligence to tailor their operations to the risks poised from overseas.

One of Secretary Johnson's earliest Departmental initiatives was directing development of a Southern Border and Approaches Campaign Planning effort that is putting together a strategic framework to further enhance the security of our southern border. The Plan will contain specific outcomes and quantifiable targets for border security and will address improved information sharing, continued enhancement and integration of sensors, and unified command and control structures as appropriate. The overall planning effort will also include a subset of campaign plans focused on addressing challenges within specific geographic areas, all with the goal of enhancing

our border security. I&A is participating in this effort to ensure threat information drives efficient use of border resources and likewise, that our border analytic focus meets the operational needs of the Department.

Countering Violent Extremism

The individualized nature of the radicalization process for homegrown violent extremists (HVEs) makes it is difficult to predict the triggers that will contribute to them attempting acts of violence. Since the Boston Marathon bombings, the Department has evolved to address the need to counter violent extremism (CVE) from an interagency perspective. Mindful of the potential for homegrown violent extremism inspired by radical ideology overseas, we continue to take steps to counter that potential threat, both through law enforcement and community outreach. Beyond the intelligence and information sharing with SLTTs and the private sector, the Department is also committed to training, through the Federal Law Enforcement Training Center, the Federal Emergency Management Agency, the National Protection and Preparedness (NPPD) Office of Infrastructure Protection and I&A. We have a commitment to training to prevent and respond to domestic attacks. Lessons learned from the Boston Marathon bombing highlighted the value in prevention and incident training.

Cybersecurity

Growing cyber threats are an increasing risk to critical infrastructure, our economy and thus, our national security. As a nation, we are faced with pervasive threats from malicious cyber actors. They are motivated by a range of reasons that include espionage, political and ideological beliefs, and financial gain. Certain nation-states pose a significant cyber threat as they aggressively target and seek access to public and private sector computer networks with the goal of stealing and exploiting massive quantities of data.

Some nation-states consistently target Government-related networks for traditional espionage, theft of protected information for financial gain, and other purposes. Increasingly, SLTT networks are experiencing nation-state cyber activity similar to that seen on federal networks. In addition to targeting government networks, there is a growing threat of nation-states targeting and compromising critical infrastructure networks and systems. Such attacks may compromise the infrastructure or control system network and provide persistent access for potential malicious cyber operations which could lead to cascading effects with physical implications.

DHS takes a customer-focused approach to information sharing, in which our desired outcome is to help prevent damaging cybersecurity incidents, such as the theft of personal information or physical disruption of critical infrastructure, and utilizes information in an operational

environment to directly reduce cybersecurity risk. DHS uses information to detect and block cybersecurity attacks on federal civilian agencies and shares information to help critical infrastructure entities in their own protection; to provide information to commercial cybersecurity companies so they can better protect their customers; and to maintain a trusted information sharing environment for private sector partners to share information and collaborate on cybersecurity threats and trends. This trust derives in large part from our emphasis on privacy, confidentiality, civil rights, and civil liberties across all information sharing programs, including special care to safeguard personally identifiable information. DHS law enforcement agencies also make substantial contributions to these cyber information sharing efforts.

I&A and NPPD work closely together every day to recognize and reduce risks posed by cyber threats. DHS' National Cybersecurity and Communications Integration Center (NCCIC) is a 24x7 operational organization that responds to, and coordinates the national response to, significant cyber incidents. NCCIC is the centralized location where federal departments and agencies, SLTT partners, private sector and international entities all form an operational nexus from which to respond. This centralized location generates collaboration and knowledge dissemination among stakeholders to provide a much greater understanding of cybersecurity vulnerabilities, intrusions, incidents, mitigation, and recovery actions.

Supporting the operational cyber mission of NPPD, I&A provides all-source analysis of cyber threats to the '.gov' domain, state and local networks, and critical infrastructure networks and systems to assist owners and operators in protecting their cyber infrastructure. I&A's cyber intelligence products and briefings are tailored to classification levels appropriate for our customers, and include For Official Use Only- and classified-level products and briefings specifically for the state and local audience.

The NCCIC actively collaborates with public and private sector partners every day, including responding to and mitigating the impacts of attempted disruptions to the Nation's critical cyber and communications networks. So far this Fiscal Year, the NCCIC has processed over 612,000 cyber incidents, issued more than 10,000 actionable cyber alerts that were used by recipients to protect their systems, detected more than 55,000 vulnerabilities through scans and assessments, and deployed 78 onsite teams for technical assistance. In one recent example, the United States Secret Service (USSS) shared information on malware observed in recent Point-of-Sale intrusions with the NCCIC for analysis. In partnership with the Financial Services Information Sharing and Analysis Center, the results of this analysis were published and enabled U.S. businesses to identify and stop ongoing cyber intrusions, thereby protecting customer data and mitigating losses.

Cybersecurity Information Sharing

While many sophisticated companies currently share cybersecurity information under existing laws, there is a continued need to increase the volume and speed of cyber threat information sharing between the government and the private sector – and among private sector entities – without sacrificing the trust of the American people or individual privacy, confidentiality, or civil liberties.

The Administration continues to take steps through executive action and public-private initiatives that incentivize and enable information sharing under existing laws. For example, Executive Order 13636 issued by President Obama in February 2013 directed intelligence agencies to increase the speed and quantity of declassified cyber threat information that the government shares with the private sector. Moreover, in February 2014, the Department of Justice and Federal Trade Commission, the two agencies charged with enforcing our antitrust laws, issued guidance that they do not believe "that antitrust is – or should be – a roadblock to legitimate cybersecurity information sharing."

While progress continues under existing law, the Administration has consistently stated that carefully updating laws to facilitate cybersecurity information sharing is one of several legislative changes essential to improve the Nation's cybersecurity. Accordingly, the Administration continues to emphasize three fundamental priorities for information sharing legislation:

1. Carefully safeguard privacy, confidentiality, and civil liberties;
2. Preserve the long-standing, respective roles and missions of civilian and intelligence agencies. Newly authorized cyber threat information sharing should enter the government through a civilian agency; and,
3. Provide for appropriate sharing with targeted liability protection.

DHS Cybersecurity Authorities

Information sharing is only one element of what is needed. We also need to update laws guiding Federal agency network security; give law enforcement the tools needed to fight crime in the digital age; create a National Data Breach Reporting requirement; and promote the adoption of cybersecurity best practices within critical infrastructure.

We urge Congress to continue efforts to modernize the Federal Information Security Management Act to reflect the existing DHS role in agencies' Federal network information security policies; clarify existing operational responsibilities for DHS in cybersecurity by authorizing the NCCIC; and provide DHS with hiring and other workforce authorities.

These provisions are vital to ensuring the Department has the tools it needs to carry out its mission.

Strengthening the Security and Resilience of Critical Infrastructure

Because the majority of the Nation's infrastructure is owned and operated by the private sector, DHS works with owners and operators, primarily on a voluntary basis, to understand evolving threats, share information on these threats and hazards, and promote best practices, training, and tools to help mitigate risks. By leveraging its core capabilities, such as information and data sharing, capacity development, vulnerability assessments, and situational awareness, DHS is effectively using its skills and resources to assist with building the Nation's resilience to physical and cybersecurity risks.

DHS works to ensure relevant information on current threats is disseminated as widely and appropriately as possible. Information sharing efforts leverage the existing partnership framework, allowing DHS to discuss threats, protective measures and joint industry/government initiatives with the private sector in order to reduce risk. For instance, DHS and FBI have engaged more than 400 major malls across the United States to facilitate 56 tabletop exercises based on a Westgate Mall, Nairobi-style attack involving coordinated active shooters and use of improvised explosive devices, and requiring a sustained response and deployment of federal resources. In addition, DHS and the Department of Energy, through the Sector Coordinating Council and in collaboration with other interagency partners, provide classified and unclassified threat briefings to CEOs and industry executives on physical and cyber threats. This frequent information sharing allows DHS and DOE to communicate specific threats to the electric sub-sector owners and operators.

The National Infrastructure Coordinating Center (NICC) maintains 24/7 situational awareness and crisis monitoring of critical infrastructure and shares threat information in order reduce risk, prevent damage, and enable rapid recovery. The NICC makes relevant information available to all critical infrastructure owners and operators through the Homeland Security Information Network, DHS's web-based information sharing platform, bringing together homeland security partners across the spectrum. Finally, the Private Sector Security Clearance Program provides a key support capability to these information sharing efforts, facilitating DHS-sponsored security clearances for critical private sector representatives across the country. This critical ability to share information at the classified level promotes a two-way exchange between the Intelligence and infrastructure protection communities that can directly lead to posturing and protection measures to mitigate risk.

Conclusion

Whether securing the Homeland from aviation threats, border threats, homegrown violent extremists, or cyber threats, DHS has matured over its tenure to recognize that it takes the intelligence, planning, training and operations of our combined components to be effective against all nefarious actors. It is through the great work and collaboration of the DHS Counterterrorism Advisory Board (CTAB) that intelligence and mitigation strategies are synthesized across the Department. The CTAB brings together the intelligence, operational and policy-making elements from across DHS to facilitate a cohesive and coordinated operational response so that DHS can deter and disrupt terrorist operations.

While many of the threats I have highlighted for you today may be emerging and evolving, the Department of Homeland Security has been poised to deal with them and remains ready to respond. Our established relationships and information sharing practices enhance our indications and warning. We continue to work closely with our partners – both here at home, as well as our international partners – to aggressively thwart plans and activities that pose a threat to the homeland. Dealing with evolving risk in a changing world is core to the DHS mission, and is carried out by an outstanding team of professionals across the globe each and every day. We will continue to evaluate and adopt serious and prudent homeland security measures as situations warrant.

Chairman Carper, Ranking Member Coburn and distinguished members of the Committee, thank you for this opportunity to testify about threats to the Homeland. We look forward to answering your questions.

Statement for the Record

The Honorable Suzanne E. Spaulding

Under Secretary, National Protection and Programs Directorate

and

The Honorable Francis X. Taylor

Under Secretary, Office of Intelligence and Analysis

U.S. Department of Homeland Security

Before the

U.S Senate Committee on Homeland Security and Governmental Affairs

Regarding

Cybersecurity, Terrorism and Beyond:

Addressing Evolving Threats to the Homeland

September 10, 2014

Introduction

Chairman Carper, Ranking Member Coburn and distinguished members of the committee, thank you for the opportunity to appear before you today to discuss terrorist, cyber and other human-caused threats to the Homeland and the current threat environment on the eve of the anniversary of the September 11, 2001 attacks.

Thirteen years later, we continue to face a dynamic threat environment. Threats to the Homeland are not limited to any one individual, group or ideology and are not defined or contained by borders. They display the increasing determination of individuals to carry out acts of terrorism that have potential to negatively impact the Homeland through loss of life, destruction of critical infrastructure, disruption of technological capabilities or services, or compromise of information security.

In the testimony today, we will highlight some of the threats we face and the risk-informed actions we take that assist government at all levels and owners and operators of critical infrastructure to understand evolving threats, share information on these threats and hazards, and promote best practices, training, and tools in the four priority areas outlined by Secretary Johnson: (1) aviation security, (2) border security, (3) countering violent extremism, and (4) cybersecurity.

Challenges Ahead

It is important to mention a couple items to provide some strategic context before covering specifics. First, the cornerstone of our mission at DHS has always been, and should continue to be, counterterrorism – that is, protecting the nation against terrorist attacks. We must remain vigilant in detecting and preventing terrorist threats that may seek to penetrate the homeland from the land, sea or air. From a security perspective, many of the resources we expend and activities we conduct apply to both countering terrorism, as well as countering transnational criminal organizations, and other homeland security challenges.

Second, to address the range of challenges the nation faces most collaboratively and effectively within the Department, we have recently undertaken an initiative entitled "Strengthening Departmental Unity of Effort." In his April 22, 2014 memorandum, Secretary Johnson directed a series of actions to enhance the cohesiveness of the Department, while preserving the professionalism, skill, and dedication of the people within, and the rich history of, the DHS components.

The actions in this initiative: new senior leader forums led by Secretary and the Deputy, and cross-departmental strategy, requirements, and budget development and acquisition processes that are tied to strategic guidance and informed by joint operational plans and joint operations are building and maturing DHS into one that is greater than the sum of its parts – one that operates

much more collaboratively, leverages shared strengths, realizes shared efficiencies, and allows us to further improve our important role as an effective domestic and international partner.

Terrorism and Aviation Security

Core Al Qa'ida, Al-Qa'ida in the Arabian Peninsula (AQAP), and their affiliates remain a major concern for DHS. Despite senior leadership deaths, the group maintains the intent and capability to conduct attacks against U.S. citizens and our facilities, and has demonstrated an ability to adjust its tactics, techniques and procedures for targeting the West in innovative ways. AQAP's three attempted attacks against the U.S. homeland—the airliner plot of December 2009, an attempted attack against U.S.-bound cargo planes in October 2010, and an airliner plot in May 2012— demonstrate their efforts to adapt to security procedures. Over the past several weeks DHS has taken a number of steps to enhance aviation security at overseas airports with direct flights to the United States, and other nations have followed with similar enhancements.

The Islamic State of Iraq and the Levant (ISIL) is a terrorist group operating as if it were a military organization, attempting to govern territory, and their experience and successes on the battlefields of Iraq and Syria have armed them with capabilities most terrorist groups do not possess. The group aspires to overthrow governments in the region and eventually beyond. At present, DHS is unaware of any specific, credible threat to the U.S. Homeland from ISIL. However, violent extremists who support them have demonstrated the intent and capability to target American citizens overseas, and ISIL constitutes an active and serious threat within the region and could attempt attacks on U.S. targets overseas with little-to-no warning. Attacks could also be conducted by supporters acting independently of ISIL direction with little-to-no warning. In January, ISIL's leader publically threatened "direct confrontation" with the United States, which is consistent with the group's media releases during the past several years that have alluded to attacking the United States.

ISIL exhibits a very sophisticated propaganda capability, disseminating high-quality media content on multiple online platforms, including social media, to enhance its appeal. ISIL's English-language messaging and its online supporters have employed—and will almost certainly continue—Twitter "hashtag" campaigns that have gained mainstream media attention and have been able to quickly reach a global audience and encourage acts of violence. Media accounts of the conflict, and propaganda in particular, play a role in inspiring U.S. citizens to travel to Syria. We are aware of a number of U.S. persons who have attempted travel to Syria this year, which underscores their continued interest in partaking in the conflict. More than 100 U.S. persons and over two thousand Westerners have traveled or attempted travel to Syria to participate in the conflict—with some of them seeking to fight with or otherwise support violent extremist groups.

We remain concerned about the threat of U.S. foreign fighters and supporters returning from Syria and whether they would to conduct attacks either on their own initiative or at the direction

of terrorist groups abroad. In addition, a small number of U.S. persons have died while fighting in Syria—including the first suicide bombing by an identified U.S. person in Syria in May and at least one other recently killed while fighting alongside ISIL. These foreign fighters, many in possession of Western passports, have likely become further radicalized while receiving additional training and experience, and pose a potential threat upon their return to their home countries.

The DHS Office of Intelligence and Analysis (I&A) is working closely with interagency partners to evaluate threat data and ensure relevant information reaches DHS personnel and state, local, tribal and territorial (SLTT) partners who can use this information to reduce risks to the Homeland. For example, I&A, the Federal Bureau of Investigation (FBI), and the National Counterterrorism Center, produced a poster, handout and muster language for DHS screeners to have background about the conflict in Syria. To ensure our SLTT and private sector partners are kept informed of the current ISIL threat, I&A has hosted multiple calls with our partners in recent months to examine the ongoing situation and, jointly with the FBI, released Joint Intelligence Bulletins (JIB) that provided context and background, examined the potential retaliatory threat and ISIL's use of social media to publicize the group's actions and goals. Following the 9/11 attacks, the importance of an informed community of first responders became clear. I&A places priority on ensuring that the Nation's first responders have the information that they need to identify the trends, tactics and behaviors of a terrorist. It also takes a vigilant public; the Department is dedicated to reminding Americans that "If You See Something, Say Something."

Border Security

Border security must include an intelligence-driven, risk-based approach that focuses resources on the places where our surveillance and intelligence tells us the threats to border security exist, and prepares us to move when the threat moves. The collaborative intelligence work of I&A, the U.S. Coast Guard, the U.S. Customs and Border Protection and the U.S. Immigration and Customs Enforcement helps keep our Southern and Northern borders safe each and every day. We ensure that the officers that are protecting the border points of entry are informed of the necessary intelligence to tailor their operations to the risks poised from overseas.

One of Secretary Johnson's earliest Departmental initiatives was directing development of a Southern Border and Approaches Campaign Planning effort that is putting together a strategic framework to further enhance the security of our southern border. The Plan will contain specific outcomes and quantifiable targets for border security and will address improved information sharing, continued enhancement and integration of sensors, and unified command and control structures as appropriate. The overall planning effort will also include a subset of campaign plans focused on addressing challenges within specific geographic areas, all with the goal of enhancing

our border security. I&A is participating in this effort to ensure threat information drives efficient use of border resources and likewise, that our border analytic focus meets the operational needs of the Department.

Countering Violent Extremism

The individualized nature of the radicalization process for homegrown violent extremists (HVEs) makes it is difficult to predict the triggers that will contribute to them attempting acts of violence. Since the Boston Marathon bombings, the Department has evolved to address the need to counter violent extremism (CVE) from an interagency perspective. Mindful of the potential for homegrown violent extremism inspired by radical ideology overseas, we continue to take steps to counter that potential threat, both through law enforcement and community outreach. Beyond the intelligence and information sharing with SLTTs and the private sector, the Department is also committed to training, through the Federal Law Enforcement Training Center, the Federal Emergency Management Agency, the National Protection and Preparedness (NPPD) Office of Infrastructure Protection and I&A. We have a commitment to training to prevent and respond to domestic attacks. Lessons learned from the Boston Marathon bombing highlighted the value in prevention and incident training.

Cybersecurity

Growing cyber threats are an increasing risk to critical infrastructure, our economy and thus, our national security. As a nation, we are faced with pervasive threats from malicious cyber actors. They are motivated by a range of reasons that include espionage, political and ideological beliefs, and financial gain. Certain nation-states pose a significant cyber threat as they aggressively target and seek access to public and private sector computer networks with the goal of stealing and exploiting massive quantities of data.

Some nation-states consistently target Government-related networks for traditional espionage, theft of protected information for financial gain, and other purposes. Increasingly, SLTT networks are experiencing nation-state cyber activity similar to that seen on federal networks. In addition to targeting government networks, there is a growing threat of nation-states targeting and compromising critical infrastructure networks and systems. Such attacks may compromise the infrastructure or control system network and provide persistent access for potential malicious cyber operations which could lead to cascading effects with physical implications.

DHS takes a customer-focused approach to information sharing, in which our desired outcome is to help prevent damaging cybersecurity incidents, such as the theft of personal information or physical disruption of critical infrastructure, and utilizes information in an operational

environment to directly reduce cybersecurity risk. DHS uses information to detect and block cybersecurity attacks on federal civilian agencies and shares information to help critical infrastructure entities in their own protection; to provide information to commercial cybersecurity companies so they can better protect their customers; and to maintain a trusted information sharing environment for private sector partners to share information and collaborate on cybersecurity threats and trends. This trust derives in large part from our emphasis on privacy, confidentiality, civil rights, and civil liberties across all information sharing programs, including special care to safeguard personally identifiable information. DHS law enforcement agencies also make substantial contributions to these cyber information sharing efforts.

I&A and NPPD work closely together every day to recognize and reduce risks posed by cyber threats. DHS' National Cybersecurity and Communications Integration Center (NCCIC) is a 24x7 operational organization that responds to, and coordinates the national response to, significant cyber incidents. NCCIC is the centralized location where federal departments and agencies, SLTT partners, private sector and international entities all form an operational nexus from which to respond. This centralized location generates collaboration and knowledge dissemination among stakeholders to provide a much greater understanding of cybersecurity vulnerabilities, intrusions, incidents, mitigation, and recovery actions.

Supporting the operational cyber mission of NPPD, I&A provides all-source analysis of cyber threats to the '.gov' domain, state and local networks, and critical infrastructure networks and systems to assist owners and operators in protecting their cyber infrastructure. I&A's cyber intelligence products and briefings are tailored to classification levels appropriate for our customers, and include For Official Use Only- and classified-level products and briefings specifically for the state and local audience.

The NCCIC actively collaborates with public and private sector partners every day, including responding to and mitigating the impacts of attempted disruptions to the Nation's critical cyber and communications networks. So far this Fiscal Year, the NCCIC has processed over 612,000 cyber incidents, issued more than 10,000 actionable cyber alerts that were used by recipients to protect their systems, detected more than 55,000 vulnerabilities through scans and assessments, and deployed 78 onsite teams for technical assistance. In one recent example, the United States Secret Service (USSS) shared information on malware observed in recent Point-of-Sale intrusions with the NCCIC for analysis. In partnership with the Financial Services Information Sharing and Analysis Center, the results of this analysis were published and enabled U.S. businesses to identify and stop ongoing cyber intrusions, thereby protecting customer data and mitigating losses.

Cybersecurity Information Sharing

While many sophisticated companies currently share cybersecurity information under existing laws, there is a continued need to increase the volume and speed of cyber threat information sharing between the government and the private sector – and among private sector entities – without sacrificing the trust of the American people or individual privacy, confidentiality, or civil liberties.

The Administration continues to take steps through executive action and public-private initiatives that incentivize and enable information sharing under existing laws. For example, Executive Order 13636 issued by President Obama in February 2013 directed intelligence agencies to increase the speed and quantity of declassified cyber threat information that the government shares with the private sector. Moreover, in February 2014, the Department of Justice and Federal Trade Commission, the two agencies charged with enforcing our antitrust laws, issued guidance that they do not believe "that antitrust is – or should be – a roadblock to legitimate cybersecurity information sharing."

While progress continues under existing law, the Administration has consistently stated that carefully updating laws to facilitate cybersecurity information sharing is one of several legislative changes essential to improve the Nation's cybersecurity. Accordingly, the Administration continues to emphasize three fundamental priorities for information sharing legislation:

1. Carefully safeguard privacy, confidentiality, and civil liberties;
2. Preserve the long-standing, respective roles and missions of civilian and intelligence agencies. Newly authorized cyber threat information sharing should enter the government through a civilian agency; and,
3. Provide for appropriate sharing with targeted liability protection.

DHS Cybersecurity Authorities

Information sharing is only one element of what is needed. We also need to update laws guiding Federal agency network security; give law enforcement the tools needed to fight crime in the digital age; create a National Data Breach Reporting requirement; and promote the adoption of cybersecurity best practices within critical infrastructure.

We urge Congress to continue efforts to modernize the Federal Information Security Management Act to reflect the existing DHS role in agencies' Federal network information security policies; clarify existing operational responsibilities for DHS in cybersecurity by authorizing the NCCIC; and provide DHS with hiring and other workforce authorities.

These provisions are vital to ensuring the Department has the tools it needs to carry out its mission.

Strengthening the Security and Resilience of Critical Infrastructure

Because the majority of the Nation's infrastructure is owned and operated by the private sector, DHS works with owners and operators, primarily on a voluntary basis, to understand evolving threats, share information on these threats and hazards, and promote best practices, training, and tools to help mitigate risks. By leveraging its core capabilities, such as information and data sharing, capacity development, vulnerability assessments, and situational awareness, DHS is effectively using its skills and resources to assist with building the Nation's resilience to physical and cybersecurity risks.

DHS works to ensure relevant information on current threats is disseminated as widely and appropriately as possible. Information sharing efforts leverage the existing partnership framework, allowing DHS to discuss threats, protective measures and joint industry/government initiatives with the private sector in order to reduce risk. For instance, DHS and FBI have engaged more than 400 major malls across the United States to facilitate 56 tabletop exercises based on a Westgate Mall, Nairobi-style attack involving coordinated active shooters and use of improvised explosive devices, and requiring a sustained response and deployment of federal resources. In addition, DHS and the Department of Energy, through the Sector Coordinating Council and in collaboration with other interagency partners, provide classified and unclassified threat briefings to CEOs and industry executives on physical and cyber threats. This frequent information sharing allows DHS and DOE to communicate specific threats to the electric sub-sector owners and operators.

The National Infrastructure Coordinating Center (NICC) maintains 24/7 situational awareness and crisis monitoring of critical infrastructure and shares threat information in order reduce risk, prevent damage, and enable rapid recovery. The NICC makes relevant information available to all critical infrastructure owners and operators through the Homeland Security Information Network, DHS's web-based information sharing platform, bringing together homeland security partners across the spectrum. Finally, the Private Sector Security Clearance Program provides a key support capability to these information sharing efforts, facilitating DHS-sponsored security clearances for critical private sector representatives across the country. This critical ability to share information at the classified level promotes a two-way exchange between the Intelligence and infrastructure protection communities that can directly lead to posturing and protection measures to mitigate risk.

Conclusion

Whether securing the Homeland from aviation threats, border threats, homegrown violent extremists, or cyber threats, DHS has matured over its tenure to recognize that it takes the intelligence, planning, training and operations of our combined components to be effective against all nefarious actors. It is through the great work and collaboration of the DHS Counterterrorism Advisory Board (CTAB) that intelligence and mitigation strategies are synthesized across the Department. The CTAB brings together the intelligence, operational and policy-making elements from across DHS to facilitate a cohesive and coordinated operational response so that DHS can deter and disrupt terrorist operations.

While many of the threats I have highlighted for you today may be emerging and evolving, the Department of Homeland Security has been poised to deal with them and remains ready to respond. Our established relationships and information sharing practices enhance our indications and warning. We continue to work closely with our partners – both here at home, as well as our international partners – to aggressively thwart plans and activities that pose a threat to the homeland. Dealing with evolving risk in a changing world is core to the DHS mission, and is carried out by an outstanding team of professionals across the globe each and every day. We will continue to evaluate and adopt serious and prudent homeland security measures as situations warrant.

Chairman Carper, Ranking Member Coburn and distinguished members of the Committee, thank you for this opportunity to testify about threats to the Homeland. We look forward to answering your questions.

Hearing before the Senate Committee on Homeland Security and Governmental Affairs
"Cybersecurity, Terrorism, and Beyond: Addressing Evolving Threats to the Homeland"
September 10, 2014

Nicholas J. Rasmussen
Deputy Director
National Counterterrorism Center

Thank you Chairman Carper, Ranking Member Coburn, and members of the Committee. I appreciate this opportunity to be here today to discuss the terrorist threat against the United States and our efforts to counter it.

I also want to express my appreciation to the Committee for its unflagging support of the men and women at the National Counterterrorism Center. I am particularly pleased to be here today with Undersecretary Taylor, Undersecretary Spaulding, and Executive Assistant Director Anderson who are representing two of our closest partner agencies—the Department of Homeland Security and the Federal Bureau of Investigation. Together we are a part of the broader counterterrorism community that is more integrated and more collaborative than ever.

Earlier this summer the 9/11 Commissioners released their most recent report, and asked national security leaders to "communicate to the public—in specific terms—what the threat is, and how it is evolving." With this in mind, Director Olsen recently had an opportunity to provide a sobering but objective assessment of Islamic State of Iraq and the Levant's (ISIL's) maturation and capability at the Brookings Institution. I similarly think hearings like this are an opportunity to continue this constructive dialogue with the public and their elected representatives.

The Overall Terrorist Threat

In May, the President told the graduating class of West Point cadets, "For the foreseeable future, the most direct threat to America at home and abroad remains terrorism." The 9/11 Commissioners agreed noting in their July report, "the terrorist threat is evolving, not defeated." From my vantage point at the National Counterterrorism Center, I would agree. Since we testified before this committee last year, the terrorist threat has evolved, is more geographically diffuse, and involves a greater diversity of actors.

Overseas, the United States faces an enduring threat to our interests, as evidenced by precautionary measures taken at some of our overseas installations. The threat emanates from a broad geographic area, spanning South Asia, across the Middle East, and much of North Africa, where terrorist networks have exploited a lack of governance and lax security.

Here in the United States, last year's attack against the Boston Marathon highlighted the danger posed by lone actors and insular groups not directly tied to terrorist organizations, as well as the difficulty of identifying these types of plots before they take place. The flow of more than 12,000 foreign fighters to Syria and Iraq with varying degrees of access to Europe and the United

States heightens our concern, as these individuals may eventually return to their home countries battle-hardened, radicalized, and willing to commit violence.

In the face of sustained counterterrorism pressure, core al-Qa'ida has adapted by becoming more decentralized and is shifting away from large-scale, mass casualty plots like the attacks of September 11, 2001. Al-Qa'ida has modified its tactics, encouraging its adherents to adopt simpler attacks that do not require the same degree of resources, training, and planning.

Instability in the Levant, Middle East, and across North Africa has accelerated this decentralization of the al-Qa'ida movement, which is increasingly influenced by local and regional factors and conditions. This diffusion has also led to the emergence of new power centers and an increase in threats by networks of like-minded violent extremists with allegiances to multiple groups. Ultimately, this less centralized network poses a more diverse and geographically dispersed threat and is likely to result in increased low-level attacks against U.S. and European interests overseas.

Today, I will begin by examining the terrorist threats to the homeland and then outline the threat to U.S. interests overseas. I will then focus the remainder of my remarks on outlining some of NCTC's efforts to address this complicated threat picture.

Threat to the Homeland

Starting with the homeland, we remain concerned about terrorist groups' efforts to target Western aviation. In early July, the United States and United Kingdom implemented enhanced security measures at airports with direct flights to the United States, which included new rules aimed at screening personal electronic devices. This past winter, additional security measures surrounding commercial aviation were implemented to address threats to the Sochi Olympics. Although unrelated, taken together these two instances are illustrative of the fact that terrorist groups continue to see commercial aviation as a desirable symbolic target, and these aspirations are not limited to Al-Qa'ida in the Arabian Peninsula.

Nevertheless, we do assess that AQAP remains the al-Qa'ida affiliate most likely to attempt transnational attacks against the United States. The group's repeated efforts to conceal explosive devices to destroy aircraft demonstrate its longstanding interest in targeting Western aviation. Its three attempted attacks demonstrate the group's continued pursuit of high-profile attacks against the West, its awareness of Western security procedures, and its efforts to adapt.

Despite AQAP's ambitions, Homegrown Violent Extremists (HVEs) remain the most likely immediate threat to the homeland. The overall level of HVE activity is likely to stay the same: a handful of uncoordinated and unsophisticated plots emanating from a pool of up to a few hundred individuals. Lone actors or insular groups who act autonomously pose the most serious HVE threat, and we assess HVEs will likely continue gravitating to simpler plots that do not require advanced skills, outside training, or communications with others.

The Boston Marathon bombing underscores the threat from HVEs who are motivated to act violently by themselves or in small groups. In the months prior to the attack, the Boston Marathon bombers exhibited few behaviors that law enforcement and intelligence officers

traditionally used to detect readiness to commit violence. The perceived success of previous lone offender attacks combined with al-Qa'ida's and AQAP's propaganda promoting individual acts of terrorism is raising the profile of this tactic.

HVEs make use of a diverse online environment that is dynamic, evolving, and self-sustaining. This online environment is likely to play a critical role in the foreseeable future in radicalizing and mobilizing HVEs towards violence. Despite the removal of important terrorist leaders during the last several years, the online environment continues to reinforce a violent extremist identity, supplies grievances, and provides HVEs the means to connect with terrorist groups overseas.

This boundless virtual environment, combined with terrorists' increasingly sophisticated use of social media, makes it increasingly difficult to protect our youth from sometimes horrifically brutal propaganda. ISIL's online media presence has become increasingly sophisticated, disseminating timely, high-quality media content across multiple platforms.

The Islamic State of Iraq and the Levant (ISIL)

ISIL is a terrorist organization that has exploited the conflict in Syria and sectarian tensions in Iraq to entrench itself in both countries. The group's strength and expansionary agenda pose an increasing threat to our regional allies and to U.S. facilities and personnel in both the Middle East and the West.

ISIL's goal is to solidify and expand its control of territory and govern by implementing its violent interpretation of *sharia* law. The group aspires to overthrow governments in the region, govern all the territory that the early Muslim caliphs controlled, and expand even further. ISIL's claim to have re-established the caliphate demonstrates the group's desire to lead violent extremists around the world.

Then Iraq-based ISIL exploited the conflict and chaos in Syria to expand its operations across the border. The group, with al-Qaida's approval, established the al-Nusrah Front as a cover for its Syria-based activities but in April 2013, publicly declared its presence in Syria under the ISIL name. ISIL accelerated its efforts to overthrow the Iraqi government, seizing control of Fallujah this past January. The group marched from its safe haven in Syria and across the border into northern Iraq, killing thousands of Iraqi Muslims on its way to seizing Mosul this June.

Along the way, ISIL aggressively recruited new adherents. Some joined ISIL to escape Assad's brutal treatment and oppression of his own people. Others joined out of frustration, marginalized by their own government. But many joined out of intimidation and fear, forced to choose either obedience to ISIL or a violent, oftentimes public death.

The withdrawal of Iraqi Security Forces during those initial military engagements has left ISIL with large swaths of ungoverned territory. It has established sanctuaries in Syria and Iraq from where they plan, train, and plot terrorist acts with little interference. Our latest assessment of ISIL's strength places the group at more than 10,000 members. Sunni groups that ISIL is

fighting with in Iraq also augment the group's strength in that battlefield. ISIL's control over the Iraq-Syria border enables the group to easily move members between Iraq and Syria, which can rapidly change the number of fighters in either country. ISIL is also drawing some recruits from the more than 12,000 foreign fighters who have traveled to Syria.

ISIL's recent victories have provided the group with a wide array of weapons, equipment, and other resources. Battlefield successes also have given ISIL an extensive war chest, which as of early this month probably includes around $1 million per day in revenues from black-market oil sales, smuggling, robberies, and ransom payments for hostages.

Notably, ISIL has sought to call into question the legitimacy of Ayman al-Zawahiri's succession of Usama bin Laden. While al-Qa'ida core remains the ideological leader of the global terrorist movement, its primacy is being challenged by the rise of ISIL whose territorial gains, increasing access to a large pool of foreign fighters, and brutal tactics are garnering significantly greater media attention. We continue to monitor for signs of fracturing within al-Qa'ida's recognized affiliates.

ISIL's safe haven in Syria and Iraq and the group's access to resources pose an immediate and direct threat to U.S. personnel and facilities in the region. This includes our embassy in Baghdad and our consulate in Erbil—and, of course, it includes the Americans held hostage by ISIL.

But ISIL's threat extends beyond the region, to the West. This January, ISIL's leader publicly threatened "direct confrontation" with the U.S., and has repeatedly taunted Americans, most recently through the horrifically graphic execution of two journalists who were reporting on the plight of the Syrian people. In Europe, the arrest of an ISIL-connected individual in France who possessed several explosive devices and a shooting in Brussels by an ISIL-trained fighter clearly demonstrate this threat, and the threat returning foreign fighters pose.

The FBI has arrested more than half a dozen individuals seeking to travel from the U.S. to Syria to support ISIL. We remain mindful of the possibility that an ISIL-sympathizer could conduct a limited, self-directed attack here at home with no warning.

Al-Qa'ida Core and Afghanistan/Pakistan-based Groups

Turning now to core al-Qa'ida and Afghanistan/Pakistan-based groups, we anticipate that despite core al-Qa'ida's diminished leadership cadre, remaining members will continue to pose a threat to Western interests in South Asia and would attempt to strike the homeland should an opportunity arise. Al-Qa'ida leader Ayman al-Zawahiri's public efforts to promote individual acts of violence in the West have increased, as the Pakistan-based group's own capabilities have diminished.

Despite ISIL's challenge, Zawahiri remains the recognized leader of the global jihadist movement among al-Qa'ida affiliates and allies, and the groups continue to defer to his guidance on critical issues. Since the start of the Arab unrest in North Africa and the Middle East,

Zawahiri and other members of the group's leadership have directed their focus there, encouraging cadre and associates to support and take advantage of the unrest.

South Asia-Based Militants. Pakistani and Afghan militant groups—including Tehrik-e Taliban Pakistan (TTP), the Haqqani Network, and Lashkar-e Tayyiba (LT)—continue to pose a direct threat to U.S. interests and our allies in the region, where these groups probably will remain focused. We continue to watch for indicators that any of these groups, networks, or individuals are actively pursuing or have decided to incorporate operations outside of South Asia as a strategy to achieve their objectives.

TTP remains a significant threat in Pakistan despite the ongoing Pakistan military operations in North Waziristan and leadership changes during the past year. Its claim of responsibility for the June attack on the Jinnah International Airport in Karachi that killed about 30 people underscores the threat the group poses inside the country.

The Haqqani network is one of the most capable and lethal terrorist groups in Afghanistan and poses a serious threat to the stability of the Afghan state as we approach 2014 and beyond. Last month, the Department of State listed four high-ranking Haqqani members—Aziz Haqqani, Khalil Haqqani, Yahya Haqqani, and Qari Abdul Rauf—on the "Rewards for Justice" most-wanted list for their involvement in terrorist attacks in Afghanistan and ties to al-Qa'ida. The Haqqanis have conducted numerous high-profile attacks against U.S., NATO, Afghan Government, and other allied nation targets. In October 2013, Afghan security forces intercepted a truck bomb deployed by the Haqqanis against Forward Operating Base Goode in the Paktiya Province. The device, which did not detonate, contained some 61,500 pounds of explosives and constitutes the largest truck bomb ever recovered in Afghanistan.

Lashkar-e-Tayyiba (LT) remains focused on its regional goals in South Asia. The group is against improving relations between India and Pakistan, and its leaders consistently speak out against India and the United States, accusing both countries of trying to destabilize Pakistan. LT has attacked Western interests in South Asia in pursuit of its regional objectives, as demonstrated by the targeting of hotels frequented by Westerners during the Mumbai attacks in 2008. LT leaders almost certainly recognize that an attack on the U.S. would result in intense international backlash against Pakistan and endanger the group's safe haven there. However, LT also provides training to Pakistani and Western militants, some of whom could plot terrorist attacks in the West without direction from LT leadership.

Al-Qa'ida Affiliates

AQAP. Al-Qa'ida in the Arabian Peninsula (AQAP) remains the affiliate most likely to attempt transnational attacks against the United States. AQAP's three attempted attacks against the United States to date—the airliner plot of December 2009, an attempted attack against U.S.-bound cargo planes in October 2010, and an airliner plot in May 2012—demonstrate the group's continued pursuit of high-profile attacks against the United States. In a propaganda video released in March, the group's leader threatened the U.S. in a speech to recruits in Yemen, highlighting AQAP's persistent interest in targeting the United States.

AQAP also presents a high threat to U.S. personnel and facilities in Yemen and Saudi Arabia. In response to credible al-Qa'ida threat reporting in August 2013, the State Department issued a global travel alert and closed U.S. embassies in the Middle East and North Africa as part of an effort to take precautionary steps against such threats. We assess that we at least temporarily delayed this particular plot, but we continue to track closely the status of AQAP plotting against our facilities and personnel in Yemen. AQAP continues to kidnap Westerners in Yemen and carry out numerous small-scale attacks and large-scale operations against Yemeni government targets, demonstrating the range of the group's capabilities. In addition, this past July AQAP launched its first successful attack in Saudi Arabia since 2009, underscoring the group's continued focus on operations in the Kingdom.

Finally, AQAP continues its efforts to radicalize and mobilize to violence individuals outside Yemen through the publication of its English-language magazine *Inspire*. Following the Boston Marathon bombings, AQAP released a special edition of the magazine claiming that accused bombers Tamarlan and Dzhokhar Tsarnaev were "inspired by *Inspire*," highlighting the attack's simple, repeatable nature, and tying it to alleged U.S. oppression of Muslims worldwide. The most recent *Inspire* issue in March—AQAP's twelfth—continued to encourage "lone offender" attacks in the West, naming specific targets in the United States, United Kingdom, and France and providing instructions on how to construct a vehicle-borne improvised explosive device.

Al-Shabaab. We continue to monitor al-Shabaab and its foreign fighter cadre as a potential threat to the U.S. homeland, as some al-Shabaab leaders have publicly called for transnational attacks and the group has attracted dozens of U.S. persons—mostly ethnic Somalis—who have traveled to Somalia since 2006. The death of al-Shabaab's leader Ahmed Abdi in a recent strike by U.S. military forces raises the possibility of potential retaliatory attacks against our personnel and facilities in East Africa.

Al-Shabaab is mainly focused on undermining the Somali Federal Government and combating African Mission in Somalia (AMISOM) and regional military forces operating in Somalia. While al-Shabaab's mid-September 2013 attack on the Westgate mall in Kenya demonstrated that the group continues to plot against regional and Western targets across East Africa, as part of its campaign to remove foreign forces aiding the Somali Government.

AQIM and regional allies. Al-Qa'ida in the Lands of the Islamic Maghreb (AQIM) and its allies remain focused on local and regional attack plotting, including targeting Western interests. The groups have shown minimal interest in targeting the U.S. homeland.

In Mali, the French-led military intervention has pushed AQIM and its allies from the cities that they once controlled, but the groups maintain safe haven in the less populated areas of northern Mali from which they are able to plan and launch attacks against French and allied forces in the region. Elsewhere, AQIM is taking advantage of permissive operating environments across much of North Africa to broaden its reach. We are concerned that AQIM may be collaborating with local violent extremists, including Ansar al-Sharia groups in Libya and Tunisia.

In August of last year, two highly capable AQIM offshoots, Mokhtar Belmokhtar's al-Mulathamun battalion and Tawhid Wal Jihad in West Africa, merged to form the new violent extremist group—al-Murabitun—which will almost certainly seek to conduct additional high profile attacks against Western interests across the region. Belmokhtar—the group's external operations commander—played a leading role in attacks against Western interests in Northwest Africa in 2013, with his January attack on an oil facility in In-Amenas, Algeria and double suicide bombings in Niger in May. Early this year, Belmokhtar relocated from Mali to Libya to escape counterterrorism pressure, and probably to collaborate with Ansar al-Sharia (AAS) and other violent extremist elements in the country to advance his operational goals.

Boko Haram is waging unprecedented violence in northeast Nigeria this year and is expanding its reach into other parts of Nigeria and neighboring states to implement its harsh version of *sharia* law and suppress the Nigerian Government and regional CT pressure. Since late 2012, Boko Haram and its splinter faction Ansaru have claimed responsibility for five kidnappings of Westerners, raising their international profile and highlighting the threat they pose to Western and regional interests. Boko Haram has kidnapped scores of additional Nigerians in northeast Nigeria since the kidnapping of 276 school girls from Chibok, Nigeria in April 2014.

Al Nusrah Front. Al-Nusrah Front is one of the most capable groups within the Syrian opposition and has mounted suicide, explosive, and firearms attacks against regime and security targets across the country; it has also sought to provide limited public services and governance to the local population in areas under its control. Several Westerners have joined al-Nusrah Front, including a few who have perished in suicide operations, raising concerns capable individuals with extremist contacts and battlefield experience could return to their home countries to commit violence. In April 2013, Al-Nusrah Front's leader, Abu Muhammad al-Jawlani, pledged allegiance to al-Qa'ida leader Ayman al-Zawahiri, publicly affirming the group's ties to core al-Qa'ida. Al-Zawahiri named the group al-Qaida's recognized affiliate in the region later last year, ordering ISIL to return to Iraq.

Al-Qa'ida in the Indian Subcontinent. This month, al-Qa'ida announced the establishment of its newest affiliate, al-Qa'ida in the Indian Subcontinent (AQIS). Al-Qa'ida used social media and online web forums to make known the existence of AQIS, which al-Qa'ida said it has worked for more than two years to create. We assess the creation of AQIS is not a reaction to al-Qa'ida's split with ISIL, though the timing of the announcement may be used to bolster al-Qa'ida's standing in the global jihad movement. AQIS, which is led by Sheikh Asim Umer, has stated objectives that include violence against the U.S., establishing Islamic law in South Asia, ending occupation of Muslim lands, and defending Afghanistan under Mullah Omar's leadership.

Threat from Shia Groups

Iran and Hizballah remain committed to defending the Assad regime, including sending billions of dollars in military and economic aid, training pro-regime and Shia militants, and

deploying their own personnel into the country. Iran and Hizballah view the Assad regime as a key partner in an "axis of resistance" against Israel and the West and are prepared to take major risks to preserve the regime as well as their critical transshipment routes.

Lebanese Hizballah. In May of last year, Hizballah publicly admitted that it is fighting for the Syrian regime and its chief, Hasan Nasrallah, framed the war as an act of self-defense against Western-backed Sunni violent extremists. Hizballah continues sending capable fighters for pro-regime operations and support for a pro-regime militia. Additionally, Iran and Hizballah are leveraging allied Iraqi Shi'a militant and terrorist groups to participate in counter-opposition operations. This active support to the Assad regime is driving increased Sunni violent extremist attacks and sectarian unrest in Lebanon.

Beyond its role in Syria, Lebanese Hizballah remains committed to conducting terrorist activities worldwide and we remain concerned the group's activities could either endanger or target U.S. and other Western interests. The group has engaged in an aggressive terrorist campaign in recent years and continues attack planning abroad. In April 2014, two Hizballah operatives were arrested in Thailand and one admitted that they were there to carry out a bomb attack against Israeli tourists, underscoring the threat to civilian centers.

Iranian Threat. In addition to its role in Syria, Iran remains the foremost state sponsor of terrorism, and works through the Islamic Revolutionary Guard Corps-Qods Force and Ministry of Intelligence and Security to support groups that target U.S. and Israeli interests globally. In March, Israel interdicted a maritime vessel that departed Iran and was carrying munitions judged to be intended for Gaza-based Palestinian militants. Iran, largely through Qods Force Commander Soleimani, has also provided support to Shia militias and the Iraqi government to combat ISIL in Iraq.

Iran continues to be willing to conduct terrorist operations against its adversaries. This is demonstrated by Iran's links to terrorist operations in Azerbaijan, Georgia, India, and Thailand in 2012. Iran also continues to provide lethal aid and support the planning and execution of terrorist acts by other groups, in particular Lebanese Hizballah.

Taken together, the current threat landscape is a manifestation of the transformation of the global jihadist movement over the past several years. This movement has diversified and expanded in the aftermath of the upheaval and political chaos in the Arab world since late 2010. The threat now comes from a more decentralized array of organizations and networks.

NCTC's Counterterrorism Efforts

The United States, United Kingdom, France, and the broader international community have increasingly expressed concerns about the greater than 12,000 foreign fighters who could potentially return to their home countries to participate in or support terrorist attacks. The UK's Home Secretary announced the terrorist threat level in the United Kingdom had been raised to severe, explaining, "The increase in threat level is related to developments in Syria and Iraq where terrorist groups are planning attacks against the West. Some of those plots are likely to

involve foreign fighters who have traveled there from the UK and Europe to take part in those conflicts."

Syria remains the preeminent location for independent or al-Qa'ida-aligned groups to recruit, train, and equip a growing number of extremists, some of whom we assess may seek to conduct external attacks. The rate of travelers into Syria exceeds the rate of travelers who went into Afghanistan/Pakistan, Iraq, Yemen, or Somalia at any point in the last ten years.

European governments estimate that more than 2,000 westerners have traveled to join the fight against the Assad regime, which includes more than 500 from Great Britain, 700 from France, and 400 from Germany. Additionally, over 100 U.S. persons from a variety of backgrounds and locations in the United States have traveled or attempted to travel to Syria.

NCTC, FBI, and DHS are part of a broader U.S. government and international effort to resolve the identities of potential violent extremists and identify potential threats emanating from Syria. As you know, this committee and the Congress charged NCTC with maintaining the U.S. government's central and shared knowledge bank of known and suspected international terrorists (or KSTs), their contacts, and their support networks. To manage this workload, NCTC developed a database called TIDE – the Terrorist Identities Datamart Environment.

TIDE is much more than a screening database – it is an analytic database. It feeds the unclassified screening database so that DHS, the State Department, and other agencies have timely and accurate information about known and suspected terrorists. As disparate pieces of information about KSTs are received, trained analysts create new records, most often as the result of a nomination by a partner agency. The records are updated—or "enhanced"—regularly as new, related information is included and dated or as unnecessary information is removed. In all cases, there are several layers of review before a nomination is accepted into the system. In the case of U.S. persons, there are at least four layers of review, including a legal review, to ensure the derogatory information is sufficient and meets appropriate standards.

To better manage and update the identities of individuals who have travelled overseas to engage in violence in Syria and Iraq, we've created a special threat case in TIDE. This is a special feature in the TIDE system which allows us to focus efforts on smaller groups of individuals. A threat case links all known actors, and their personal information, involved in a particular threat stream or case and makes that information available to the intelligence, screening, and law enforcement communities.

NCTC's management of this unique consolidation of terrorist identities has created a valuable forum for identifying and sharing information about Syrian foreign fighters—including ISIL—with community partners. It has better integrated the community's efforts to identify, enhance, and expedite the nomination of Syrian foreign fighter records to the Terrorist Screening Database for placement in U.S. government screening systems.

Counterterrorism efforts focused on law enforcement disruptions are critical to mitigating threats. We also recognize that government alone cannot solve this problem and interdicting or arresting terrorists is not the full solution. Well-informed and well-equipped families,

communities, and local institutions represent the best long-term defense against violent extremism.

To this end, we continue to refine and expand the preventive side of counterterrorism. Working with DHS, in the last year NCTC revamped the Community Awareness Briefing (CAB), a key tool we use to convey information to local communities and authorities on the terrorist recruitment threat. The CAB now also includes information on the recruitment efforts of violent extremist groups based in Syria and Iraq. Additionally, this year NCTC and DHS developed and implemented a new program – the Community Resilience Exercise program, designed to improve communication between law enforcement and communities and to share ideas on how to counter violent extremism.

Conclusion

Confronting these threats and working with resolve to prevent another terrorist attack remains the counterterrorism community's overriding mission. This year, NCTC celebrates its 10th year in service to the nation, and while the Center has matured tremendously over that period, we are focused on positioning ourselves to be better prepared to address the terrorist threat in decades to come.

Chairman Carper, Ranking Member Coburn, and members of the Committee, thank you for the opportunity to testify before you this morning. I want to assure you that our attention is concentrated on the security crises in Iraq and Syria—and rightly so. But we continue to detect, disrupt, and defeat threats from across the threat spectrum.

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

Department of Justice

STATEMENT OF

ROBERT ANDERSON, JR.
EXECUTIVE ASSISTANT DIRECTOR
CRIMINAL, CYBER, RESPONSE, AND SERVICES BRANCH
FEDERAL BUREAU OF INVESTIGATION
DEPARTMENT OF JUSTICE

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

ENTITLED

"CYBERSECURITY, TERRORISM, AND BEYOND:
ADDRESSING EVOLVING THREATS TO THE HOMELAND"

PRESENTED

SEPTEMBER 10, 2014

Statement of
Robert Anderson, Jr.
Executive Assistant Director
Criminal, Cyber, Response, and Services Branch
Federal Bureau of Investigation
Department of Justice

Before the
Committee on Homeland Security and Governmental Affairs
United States Senate

Entitled
"Cybersecurity, Terrorism, and Beyond: Addressing Evolving Threats to the Homeland"

Presented on
September 10, 2014

Good morning Chairman Carper and Ranking Member Coburn. I appreciate the opportunity to appear before you today to discuss cyber, terrorism, and other threats to our nation and how the FBI is collaborating with our partners in government, law enforcement, and the private sector to prevent and combat them.

The Cyber Threat and FBI Response

We face cyber threats from state-sponsored hackers, hackers for hire, global cyber syndicates, and terrorists. They seek our state secrets, our trade secrets, our technology, and our ideas—things of incredible value to all of us. They seek to strike our critical infrastructure and to harm our economy.

Given the scope of the cyber threat, agencies across the Federal government are making cyber security a top priority. We and our partners at the Department of Homeland Security (DHS), the National Security Agency, and other U.S. Intelligence Community and law enforcement agencies have truly undertaken a whole-of-government effort to combat the cyber threat. Within the FBI, we are prioritizing high-level intrusions—the biggest and most dangerous botnets, state-sponsored hackers, and global cyber syndicates. We are working with our counterparts to predict and prevent attacks, rather than simply react after the fact.

FBI agents, analysts, and computer scientists use technical capabilities and traditional investigative techniques—such as sources and wiretaps, surveillance, and forensics—to fight cyber crime. We work side-by-side with our Federal, State, and local partners on Cyber Task Forces in each of our 56 field offices and at the National Cyber Investigative Joint Task Force (NCIJTF). Through our 24-hour cyber command center, CyWatch, we combine the resources of the FBI and NCIJTF, allowing us to provide connectivity to Federal cyber centers, government

agencies, FBI field offices and legal attachés, and the private sector in the event of a significant cyber intrusion.

We also exchange information about cyber threats with the private sector through partnerships such as the Domestic Security Alliance Council, InfraGard, and the National Cyber Forensics and Training Alliance (NCFTA).

For our partners in State and local law enforcement, we have launched Cyber Shield Alliance on www.leo.gov, which provides access to cyber training opportunities and information, as well as the ability to report cyber incidents to the FBI.

In addition, our legal attaché offices overseas work to coordinate cyber investigations and address jurisdictional hurdles and differences in the law from country to country. We are supporting and collaborating with newly established cyber crime centers at Interpol and Europol. We continue to assess other locations to ensure that our cyber personnel are in the most appropriate locations across the globe

We know that to be successful in the fight against cyber crime, we must continue to recruit, develop, and retain a highly skilled workforce. To that end, we have developed a number of innovative staffing programs and collaborative private industry partnerships to ensure that over the long term we remain focused on our most vital resource—our people.

As the committee is well aware, the frequency and impact of cyber attacks on our nation's private sector and government networks have increased dramatically in the past decade, and are expected to continue to grow. Since 2002, the FBI has seen an 80 percent increase in the number of computer intrusion investigations.

Recent Successes

Over the past several months, the FBI and the Justice Department have announced a series of separate indictments of overseas cyber criminals.

In an unprecedented indictment in May, we charged five Chinese hackers with illegally penetrating the networks of six U.S. companies. The five members of China's People's Liberation Army allegedly used their illegal access to exfiltrate proprietary information, including trade secrets.

Later that month, we announced the indictments of a Swedish national and a U.S. citizen believed to be the co-developers of a particularly insidious computer malware known as Blackshades. This software was sold and distributed to thousands of people in more than 100 countries and has been used to infect more than half a million computers worldwide.

In June, the FBI announced a multinational effort to disrupt the GameOver Zeus botnet, the most sophisticated botnet that the FBI and its allies had ever attempted to disrupt. GameOver Zeus is believed to be responsible for the theft of millions of dollars from businesses and consumers in the U.S. and around the world. This effort to disrupt it involved notable cooperation with the

private sector and international law enforcement. GameOver Zeus is an extremely sophisticated type of malware designed specifically to steal banking and other credentials from the computers it infects. In the case of GameOver Zeus, its primary purpose is to capture banking credentials from infected computers, then use those credentials to initiate or re-direct wire transfers to accounts overseas that are controlled by the criminals. Losses attributable to GameOver Zeus are estimated to be more than $100 million.

Just last month, a Federal grand jury indicted Su Bin, a Chinese national, on five felony offenses stemming from a computer hacking scheme that involved the theft of trade secrets from American defense contractors, including The Boeing Company, which manufactures the C-17 military transport aircraft. Su is currently in custody in British Columbia, Canada, where he is being held pursuant to a provisional arrest warrant submitted by the United States. The charges carry a total maximum statutory penalty of 30 years in prison. The investigation in this case was conducted by the Federal Bureau of Investigation and the Air Force Office of Special Investigations.

The Blackshades and GameOver Zeus indictments are part of an initiative launched by the FBI Cyber Division in April 2013 to disrupt and dismantle the most significant botnets threatening the economy and national security of the United States. This initiative, named Operation Clean Slate, is the FBI's broad campaign to implement appropriate threat neutralization actions through collaboration with the private sector, DHS, and other United States government partners, as well as our foreign partners. This includes law enforcement action against those responsible for the creation and use of the illegal botnets, mitigation of the botnet itself, assistance to victims, public service announcements, and long-term efforts to improve awareness of the botnet threat through community outreach. Although each botnet is unique, Operation Clean Slate's strategic approach to this significant threat ensures a comprehensive neutralization strategy, incorporating a unified public/private response and a whole-of-government approach to protect U.S. interests.

The impact of botnets has been significant. Botnets have been estimated to cause more than $113 billion in losses globally, with approximately 375 million computers infected each year, equaling more than one million victims per day, translating to 12 victims per second.

Another Operation Clean Slate success came in January 2014, when Aleksandry Andreevich Panin, a Russian national, pled guilty to conspiracy to commit wire and bank fraud for his role as the primary developer and distributor of the malicious software known as Spyeye, which infected more than 1.4 million computers in the United States and abroad. Based on information received from the financial services industry, more than 10,000 bank accounts had been compromised by Spyeye infections in 2013 alone. Panin's co-conspirator, Hamza Bendelladj, an Algerian national who helped Panin develop and distribute the malware, was also arrested in January 2013 in Bangkok, Thailand.

In addition to these recent investigative successes against cyber threats, we are continuing to work with our partners to prevent attacks before they occur.

One area in which we have had great success with our overseas partners is in identifying and targeting infrastructure we believe has been used in distributed denial of service (DDoS) attacks,

and preventing that infrastructure from being used for future attacks. A DDoS attack is an attack on a computer system or network that causes a loss of service to users, typically the loss of network connectivity and services by consuming the bandwidth of the victim network.

Since October 2012, the FBI and DHS have released more than 170,000 Internet Protocol addresses of computers that were believed to be infected with DDoS malware. We have released this information through Joint Indicator Bulletins (JIBs) to more than 130 countries via DHS's National Cybersecurity and Communications Integration Center (NCCIC), where our liaisons provide expert and technical advice for increased coordination and collaboration, as well as to our legal attachés overseas.

These actions have enabled our foreign partners to take action and reduced the effectiveness of the botnets and the DDoS attacks. We are continuing to target botnets through this strategy and others.

In 2013, for example, the FBI created FBI Liaison Alert System (FLASH) reports and Private Industry Notifications (PINs) to release industry-specific details on current and emerging threat trends, and technical indicators to the private sector. To date, the FBI has disseminated 40 FLASH messages, 21 of which dealt with threats to the financial industry. These PIN and FLASH messages were created to proactively deliver timely, actionable intelligence to potential victims and law enforcement partners at the international, State, and local levels.

Next Generation Cyber Initiative

The need to prevent attacks is a key reason the FBI has redoubled our efforts to strengthen our cyber capabilities while protecting privacy, confidentiality, and civil liberties. The FBI's Next Generation Cyber Initiative, which we launched in 2012, entails a wide range of measures, including focusing the Cyber Division on intrusions into computers and networks—as opposed to crimes committed with a computer as a modality hiring additional computer scientists to assist with technical investigations in the field; and expanding partnerships and collaboration at the NCIJTF. In addition, after more than a decade of combating cybercrime through a nationwide network of interagency task forces, the FBI has evolved its Cyber Task Forces in all 56 field offices to focus exclusively on cybersecurity threats.

At the NCIJTF—which serves as a coordination, integration, and information sharing center for 19 U.S. agencies and several key international allies for cyber threat investigations—we are coordinating at an unprecedented level. This coordination involves senior personnel at key agencies. NCIJTF, which is led by the FBI, now has deputy directors from the NSA, DHS, the Central Intelligence Agency, U.S. Secret Service, and U.S. Cyber Command. In the past year, three of our Five Eyes international partners joined us at the NCIJTF: Australia embedded a liaison officer in May 2013, the UK in July 2013, and Canada in January 2014. By developing partnerships with these and other nations, NCIJTF is working to become the international leader in synchronizing and maximizing investigations of cyber adversaries.

Private Sector Outreach

In addition to strengthening our partnerships in government and law enforcement, we recognize that to effectively combat the cyber threat, we must significantly enhance our collaboration with the private sector. Our nation's companies are the primary victims of cyber intrusions, and their networks contain the evidence of countless attacks. In the past, industry has provided us information about attacks that have occurred, and we have investigated the attacks—but we have not always provided information back.

To remedy that, the Cyber Division has established a Key Partnership Engagement Unit (KPEU) to manage a targeted outreach program focused on building relationships with key private sector corporations. The unit works to share sector-specific threat information with our corporate partners.

We have provided a series of classified briefings for key sectors, including financial services and energy, to help them repel intruders.

Through the FBI's InfraGard program, the FBI develops partnerships and working relationships with private sector, academic, and other public-private entity subject matter experts. Primarily geared toward the protection of critical national infrastructure, InfraGard promotes ongoing dialogue and timely communication among a current active membership base of more than 25,000.

InfraGard members are encouraged to share information with government that better allows government to prevent and address criminal and national security issues. Active members are able to report cyber intrusion incidents in real-time to the FBI through iGuardian, which is based on our successful counterterrorism reporting system known as Guardian.

Just last month, the FBI deployed a malware repository and analysis system called Malware Investigator to our domestic and foreign law enforcement partners and members of the U.S. Intelligence Community. The system allows users to submit malware directly to the FBI and quickly receive technical information about the samples to its users so they can understand how the malware works. It also enables the FBI to obtain a global view of the malware threat. Beyond technical reporting, Malware Investigator identifies correlations that will allow users to "connect the dots" by highlighting instances in which malware was deployed in seemingly unrelated incidents.

The FBI's Cyber Initiative and Resource Fusion Unit (CIRFU) maximizes and develops intelligence and analytical resources received from law enforcement, academia, international, and critical corporate private sector subject matter experts to identify and combat significant actors involved in current and emerging cyber-related criminal and national security threats. CIRFU's core capabilities include a partnership with the National Cyber Forensics and Training Alliance (NCFTA) in Pittsburgh, Pennsylvania, where the unit is collocated with CIRFU. NCFTA acts as a neutral platform through which the unit develops and maintains liaison with hundreds of formal and informal working partners who share real-time threat information and

best practices and collaborate on initiatives to target and mitigate cyber threats domestically and abroad.

The FBI recognizes that industry collaboration and coordination are critical in our combating the cyber threat effectively. As part of our enhanced private sector outreach, we have begun to provide cleared industry partners with classified threat briefings and other information and tools to better help them repel intruders.

Counterterrorism and Other Threats

Though the cyber threat is one of the FBI's top priorities, combating terrorism remains our top investigative priority. As geopolitical conflict zones continue to emerge throughout many parts of the world, terrorist groups may use this instability to recruit and incite acts of violence.

The continuing violence in both Syria and Iraq and the influx of foreign fighters threatens to destabilize an already volatile region while also heightening the threat to the West. Due to the prolonged nature and the high visibility of the Syrian conflict, we are concerned that U.S. persons with an interest in committing jihad will be drawn to the region. We can address this issue more fully in the closed session.

***

In conclusion, Chairman Carper, to counter the threats we face, we are engaging in an unprecedented level of collaboration within the U.S. government, with the private sector, and with international law enforcement.

We are grateful for the committee's support and look forward to continuing to work with you and expand our partnerships to defeat our adversaries.