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.