FINAL

Prepared Testimony on "Worldwide Threats and Homeland Security Challenges"

Secretary of Homeland Security Jeh Charles Johnson

House Committee on Homeland Security

October 21, 2015

Chairman McCaul, Representative Thompson, and members of the Committee, thank you for the opportunity to be here. I welcome the opportunity to appear before you with Directors Comey and Rasmussen to discuss threats to the homeland and what we are doing to address them. Though I am prepared to discuss the full scope of DHS missions, in these prepared remarks I will focus on: (i) counterterrorism, (ii) aviation security, and (iii) cybsersecurity.

Counterterrorism

Last month, I attended a sobering ceremony in Shanksville, Pennsylvania for the 14th anniversary of 9/11. Today, 14 years after 9/11, it is still a dangerous world.

The events on 9/11 were the most prominent and devastating example of terrorist attacks by those who are recruited, trained and directed overseas, and exported to our homeland. The 9/11 hijackers were acting on orders from al Qaeda's external operations chief, Khalid Sheikh Mohammed, who was in turn carrying out the direction of Osama bin Laden.

Likewise, the attempted "Shoe Bomber" in December 2001, the attempted "Underwear Bomber" in December 2009, the attempted Times Square car bombing in May 2010, and the attempted "Package Bomb" plot in October 2010, were all efforts to export terrorism to the United States, and they all appear to have been directed by a terrorist organization overseas.

The response to these types of attacks and attempted attacks on our homeland was and is to take the fight directly to the terrorist organizations at locations overseas.

But, today the global terrorist threat is more decentralized, more complex, and in many respects harder to detect. The new reality involves the potential for smaller-scale attacks by those who are either homegrown or home-based, not exported, and who are inspired by, not necessarily directed by, a terrorist organization.

Today, it is no longer necessary for terrorist organizations to personally recruit, train, and direct operatives overseas and in secret, and export them to the U.S. to commit a terrorist attack. Today, with new and skilled use of the internet, terrorist organizations may publicly recruit and inspire individuals to conduct attacks within their own homelands. Al Qaeda in the Arabian Peninsula no longer hides the fact that it builds

bombs; it publicizes its instruction manual in its magazine, and publicly urges people to use it.

Today, we are also concerned about foreign terrorist fighters who are answering public calls to leave their home countries in Europe and elsewhere to travel to Iraq and Syria and take up the extremists' fight there. Many of these individuals will seek to return to their home countries with that same extremist motive.

On September 29, this Committee's bipartisan task force published a report on foreign terrorist fighters. I would like to thank the Committee, in particular Chairman McCaul and Ranking Member Thompson, for your work on this important assessment of how we in the U.S. Government can enhance our efforts to counter the threat of foreign terrorist fighters. As noted in the report, the Department of Homeland Security has undertaken much of what is recommended. We have been and are continuing to institute measures to detect and prevent travel by foreign terrorist fighters.

The recent wave of terrorist attacks and attempted attacks here and in Europe reflect the new reality of the global terrorist threat. The Boston Marathon bombing in April 2013, the attack on the war memorial and the parliament building in Ottawa in October 2014, the attack on the Charlie Hebdo headquarters in Paris in January 2015, the attempted attack in Garland City, Texas in May 2015, and the attack that killed five U.S. service members in Chattanooga, Tennessee in July: What does this recent wave of attacks and attempted attacks have in common? They were all conducted by homegrown or home-based actors, and they all appear to have been inspired, but not directed by, al Qaeda or ISIL.

Finally, we are concerned about domestic terrorism in the form of a "lone wolf" which can include various aspects of domestic terrorism such as right-wing extremism. We devote substantial efforts to study and understand these threats and will continue to further our understanding of the underpinnings of terrorist threats of all forms.

So, what are we doing about it?

The Department of Homeland Security, following the attacks in Ottawa, Canada last October, and in reaction to terrorist groups' public calls for attacks on government installations in the West, directed the Federal Protective Service to enhance its presence and security at various United States Government buildings in Washington, DC and other major cities and locations around the country. We continue this enhanced presence today.

There are presently 38 countries from which we do not require a visa to travel here. This "Visa Waiver Program" is a valuable program to promote trade and travel with our most valued allies. Last November, I directed that, for security reasons, we add

fields to the Electronic System for Travel Authorization, or "ESTA" system that travelers from these countries are required to use.

In August 2015, we introduced further security enhancements to the Visa Waiver Program. From now on, countries in the Program will be required to, among other actions, implement arrangements to share information about known and suspected terrorists and serious criminals; collect and analyze travel data; and cooperate with INTERPOL – both for using INTERPOL's Lost and Stolen Passport Database to screen travelers crossing a VWP's country's borders, as well as reporting foreign fighters to multilateral organizations such as INTERPOL or EUROPOL. We also requested permission for the expanded use of U.S federal air marshals on international flights from VWP countries to the U.S. These security enhancements will enable us to learn more about travelers from visa waiver countries and to more accurately and effectively identify those who pose a security risk before they board planes bound for the United States. These enhancements have already produced tangible security benefits.

Next, given the new reality of the global terrorist threat – which involves the potential for small-scale homegrown attacks by those who could strike with little or no notice -- we are enhancing our collaboration with state and local law enforcement. Almost every day, DHS and the FBI share intelligence and pertinent terrorist threat information with Joint Terrorism Task Forces, state fusion centers, local police chiefs and sheriffs. We have also enhanced our information sharing with businesses and critical infrastructure.

With regard to the current refugee crisis, the U.S. is committed to providing refuge to some of the world's most vulnerable people, while carefully screening refugees for security concerns before admitting them to the United States. The reality is that, with improvements to the process we have made over time, refugees are subject to the highest level of security checks. DHS works in concert with the Department of State, the Department of Defense, the National Counterterrorism Center, and the FBI's Terrorist Screening Center for the screening and vetting of refugees. The U.S. Government conducts both biographic and biometric checks on refugee applications, including security vetting that takes place at multiple junctures in the application process, and even just before arrival to account for changes in intelligence. All refugees admitted to the United States, including those from Syria, will be subject to this stringent security screening. Acting on my direction, USCIS has developed additional protocols to aid in the identification of security concerns with regard to the Syrian population, and the entire Department, along with the interagency, is committed to conintual improvement of overall security vetting, as new techniques or sources of information are identified.

Next, given the nature of the evolving terrorist threat, countering violent extremism in this country is as important as any of our other key missions. Building trusted partnerships with diverse communities is essential to successfully countering

violent extremism and curbing threats to the safety of our country. These communities must be empowered to reach those individuals most susceptible to the slick internet appeal of ISIL before they turn to violence. In the last Fiscal Year, DHS held close to 200 meetings, roundtables, and other events in 14 cities in which I participated. And, since becoming Secretary, I have personally met with community leaders in Chicago, Columbus, Minneapolis, Los Angeles, Boston, New York City, Houston, suburban Maryland, and northern Virginia.

We are now taking our CVE efforts to the next level. On September 28th, I announced a new DHS Office for Community Partnerships which builds upon the ongoing CVE work across the Department, consolidates our efforts, and takes them to the next level. This office will be the central hub for the Department's efforts to counter the evolving global terrorist threat to our country. I named Mr. George Selim as the Director of this Office. George brings significant experience to his new role, having served as the Director for Community Partnerships for the National Security Council since 2012 and previously worked at the DHS Office of Civil Rights and Civil Liberties.

My objectives for this Office are to build upon our partnerships with state and local communities and governments, coordinate and promote relationship building efforts inside and outside of government, identify resources to support countering violent extremism through government-funded grants, public-private partnerships, technology, and philanthropy. Meanwhile, the DHS Office for Civil Rights and Civil Liberties will partner with the Office of Community Partnerships and lead, improve, and expand its important community engagement work, including Community Engagement Roundtables, Town Hall Meetings, and Youth Forums, in cities all across the country.

Finally, our homeland security efforts must also involve public vigilance and action. At the Super Bowl earlier this year, I re-launched the "If You See Something, Say Something™" public awareness campaign with the National Football League to help ensure the safety and security of employees, players, and fans during Super Bowl XLIX. The newly revamped materials highlight the individual role of everyday citizens to protect their neighbors and the communities they call home by recognizing and reporting suspicious activity. "If You See Something, Say Something ™" is more than a slogan. The public must play an important role in keeping our neighborhoods and communities safe.

Aviation security

Since last summer, I have required enhanced screening at select overseas airports with direct flights to the United States. The United Kingdom and other countries have followed suit with similar enhancements, and the European Union passed legislation for both near and long-term enhancements to cabin baggage screening requirements.

Earlier this year in response to a December incident at the Hartfield-Jackson-Atlanta airport, I asked the Aviation Security Advisory Committee (ASAC) to review and make recommendations to address concerns about whether aviation workers with airport identification badges could bypass security and smuggle weapons or explosives into an operations area or even onto an aircraft. In April, in response to the ASAC's recommendations, I directed the Transportation Security Administration (TSA) to take several immediate actions, including "real-time recurrent" criminal history background checks coordinated with the FBI, reducing the number of access points to secured areas, and encouraging airport workers to report suspicious activity.

I have also prioritized the expansion of preclearance operations at foreign airports with flights to the United States. Preclearance allows U.S. Customs and Border Protection officers overseas to screen passengers bound for the United States at the front end of the flight, protecting the plane, its passengers, and our country, before they even enter the United States. We now have 15 preclearance sites overseas, in 6 different countries, operated by more than 600 CBP officers and agriculture specialists. The most recent preclearance operation was set up early last year in Abu Dhabi. Since that time, in Abu Dhabi alone, we have already inspected more than 580,000 passengers and crew bound for the United States, and have determined 1002 individuals to be inadmissible, including a number of them based on national security related grounds. We are in active negotiations with several countries to expand preclearance operations to ten new foreign airports. I view preclearance as an important piece of our aviation security and our counterterrorism mission.

In May, the classified, preliminary results of the DHS Inspector General's tests of TSA's screening at airports were leaked to the press. The OIG completed its classified report last month, and has provided it to the Department and to Congress. The final report recommends corrective measures that TSA is already undertaking. In May and June, I directed a series of actions constituting a 10-point plan to address the concerns raised by the OIG's testing. This plan included a number of immediate and longer-term measures. Under the new leadership of Admiral Peter Neffenger, TSA has promptly begun increasing manual screening and random explosive trace detectors, re-testing and re-evaluating the type of screening equipment tested by the OIG, revising standard operating procedures, and conducting "back to basics" training for every TSA officer in the country. Many of these measures have either been completed, or soon will be.

Cybersecurity

Cybersecurity is critical to homeland security. Cybersecurity is a top priority for me, the President, and this Administration.

To be frank, our federal .gov cybersecurity, in particular, is not where it needs to be. In the case of the breach of the Office of Personnel Management, a large amount of

highly personal and sensitive information was taken by a very sophisticated actor. There is a great deal that has been done and is being done now to secure our networks. We do, in fact, block a large number of intrusions and exfiltrations, including those by state actors. But much more must be done.

By law, each head of a federal department or agency is primarily responsible for his or her agency's own cybersecurity. DHS has overall responsibility for protecting federal civilian systems from cyber threats, helping agencies better defend themselves, and providing response teams to assist agencies during significant incidents. We have also been able to use the unique authorities given to us by Congress to engage with the critical infrastructure community to reduce the risk that our essential services and functions could be disrupted by a cyber attack.

DHS's National Cybersecurity and Communications Integration Center, or "NCCIC," is the U.S. government's 24/7 hub for cybersecurity information sharing, incident response, and coordination. Thirteen federal departments and agencies and 16 private sector entities have regular, dedicated liaisons at the NCCIC, while over 100 private sector entities collaborate and share information with the NCCIC on a routine basis.

The NCCIC shares information on cyber threats and incidents, and provides on-site assistance to victims of cyberattacks. In this fiscal year alone, the NCCIC has shared over 15,000 bulletins, alerts, and warnings, responded on-site to 21 incidents and conducted nearly 130 technical security assessments.

It is my personal mission to significantly enhance the Department's role in the cybersecurity of our government and the Nation. To achieve this, I have directed the accelerated and aggressive deployment of important technologies, guidance, and partnerships that my Department is uniquely situated to provide.

First, we have prioritized full deployment of our EINSTEIN system: an intrusion detection and prevention system that uses classified information to protect unclassified networks. I have directed the National Protection and Programs Directorate to make at least some EINSTEIN 3A countermeasures available to all federal civilian departments and agencies no later than December 31, 2015. We are currently on schedule to achieve this goal. We have also successfully expanded our private sector version of this program – Enhanced Cybersecurity Services – to all critical infrastructure sectors.

EINSTEIN has demonstrated its value. Since its introduction, E3A has blocked over 650,000 requests to access potentially malicious websites. These attempts are often associated with adversaries who are already on federal networks attempting to communicate with their "home base" and steal data from agency networks. Importantly, EINSTEIN 3A is also a platform for future technologies and capabilities to do

more. This includes technology that will automatically identify suspicious Internet traffic for further inspection, even if we did not already know about the particular cybersecurity threat.

Second, DHS helps federal agencies identify and fix problems in near-real-time using Continuous Diagnostics and Mitigation programs – or "CDM." Once fully deployed, CDM will monitor agency networks internally for vulnerabilities that could be exploited by bad actors that have breached the perimeter. CDM will allow agencies to identify, prioritize, and fix the most significant problems first. It will also provide DHS with situational awareness about government-wide risk for the broader cybersecurity mission.

Earlier this year, I directed that NPPD make the first phase of CDM available to 97% of federal civilian departments and agencies by September 30, 2015. We achieved this goal ahead of schedule and are on track to make the second phase available by the end of Fiscal Year 2016.

Third, information sharing is fundamental to achieving our mission. We must be able to share information in as close to real time as possible while ensuring appropriate privacy protections. We have made excellent progress by leading the development of a system that makes automated information sharing possible. By November, we will have the capability to automate the distribution and receipt of cyber threat indicators. Our partners in the Intelligence Community and law enforcement have participated in the development of this capability and support the policies that we have put in place to ensure that we have both appropriate privacy protections and the quick dissemination of relevant information to other agencies.

We are working closely with other agencies of our government to support the stand-up of the ODNI-led Cyber Threat Intelligence Integration Center, or "CTIIC." This is vital because the foreign cyber threats we face as a Nation are too many, too sophisticated and increasingly too severe to wait any longer to ensure we integrate the intelligence about cyber threats to better inform our defenses and our actions – just as we do with regard to terrorist threats. DHS looks forward to full implementation of this Intelligence Community initiative, which will help all of the operational cyber centers better understand various strategic cyber threats and provide improved intelligence community support to the NCCIC, which will, in turn, enable us to share more information with our private sector partners.

Last month, we participated in frank discussions with officials of the People's Republic of China on cyber issues of concern to both our nations. This culminated in our Presidents announcing several key cybersecurity commitments. As part of these commitments, we agreed to investigate cyber crimes, collect electronic evidence, and mitigate malicious cyber activity emanating from its territory, and to provide timely

responses to requests for information and assistance concerning those activities. Both sides also agreed to provide updates on the status and results of those investigations and to take appropriate action. As part of this commitment, we agreed to establish a high-level joint dialogue mechanism on fighting cybercrime and related issues. Perhaps most importantly, the United States and China committed that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors. The United States and China also committed to create a senior experts group on international security issues in cyberspace.

Time will tell whether the Chinese will live up to these commitments. I intend to remain personally engaged on these issues, to ensure that China takes concrete steps to advance progress made thus far. To be sure, these commitments do not resolve all our challenges with China on cyber issues. But, they do represent a step forward in our efforts to address one of the sharpest areas of disagreement in the U.S.-China bilateral relationship. On the U.S. side, we are prepared to fulfill our commitments. Words must be matched by actions.

We cannot detect and stop every cyber single intrusion. So often, the most sophisticated actors penetrate the gate through a simple act of spearphishing, because they know they can count on a single user letting his guard down. But, we have made considerable progress and continue to take aggressive action.

I urge Congress to act by passing cyber legislation. I applaud the bipartisan work that has been done so far in this Congress. We need legislation to accomplish at least two things:

First, we need explicit congressional authorization of the EINSTEIN program. This would eliminate any remaining legal obstacles to its deployment across the Federal Government. The House has passed H.R. 1731, which accomplishes this and ensures agencies understand they are legally permitted to disclose network traffic to DHS for narrowly tailored purposes.

Second, we need the Senate to finish its work on the Cybersecurity Information Sharing Act as soon as possible. This Committee's engagement with the bill's sponsors has strengthened the legislation and incorporated important modifications to better protect privacy. I understand that work continues to make necessary changes, and we greatly appreciate those efforts. But cyber criminals are not waiting to steal intellectual property or financial data, so neither can Congress wait to pass information sharing legislation. I urge you to call upon Senate leadership to bring this bill up as soon as possible so that the Senate can finish its work and pass it.

Conclusion

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

Thank you, and I look forward to your questions.