

Prepared Testimony

**Secretary of Homeland Security Jeh Charles Johnson
U.S. Senate
Committee on Homeland Security and Governmental Affairs**

“Fifteen Years after 9/11: Threats to the Homeland”

September 27, 2016

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

Counterterrorism

Today, 15 years after 9/11, it is still a dangerous world. Recent events in New York City, New Jersey, Minnesota, San Bernardino and Orlando are terrible reminders of the new threats we face to the homeland.

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

The events on September 17 illustrate the serious threat of homegrown violent extremism.

This threat environment has required a whole new type of response and we are aggressively strengthening and building more capabilities to respond.

As directed by President Obama, our government, along with our coalition partners, continues to take the fight militarily to terrorist organizations overseas. ISIL is the terrorist organization most prominent on the world stage. Since September 2014, air strikes and special operations have in fact led to the death of a number of ISIL's leaders and those focused on plotting external attacks in the West. At the same time, ISIL has lost about 49% of the populated areas it once controlled in Iraq, and thousands of square miles of territory it once controlled in Syria. But as ISIL loses territory, it has increased

UNCLASSIFIED

its plotting on targets outside of Iraq and Syria, and continues to encourage attacks in the United States.

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

Following the attacks in Ottawa, Canada in 2014, and in reaction to terrorist groups' public calls for attacks on government installations in the western world, I directed the Federal Protective Service to enhance its presence and security at various U.S. government buildings around the country.

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

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

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

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

We are strengthening the security of our Visa Waiver Program, which permits travelers from 38 different countries to come to the U.S. for a limited time period without a visa. In 2014, we began to collect more personal information in the Electronic System

for Travel Authorization, or “ESTA” system, that travelers from Visa Waiver countries are required to use. ESTA information is screened against the same counterterrorism and law enforcement databases that travelers with traditional visas are screened, and must be approved prior to an individual boarding a plane to the United States. As a result of these enhancements, since 2014, over 3500 additional travelers were denied visa-free travel here through this program. In August 2015, we introduced further security enhancements to the Visa Waiver Program.

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

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

CBP is deploying personnel at various airports abroad, to pre-clear air travelers before they get on flights to the United States. At present, we have this pre-clearance capability at 15 airports overseas. And, last year, through pre-clearance, we denied boarding to over 10,700 travelers (or 29 per day) before they even got to the United States. As I said here last year, DHS intends to expand the pre-clearance program. In May 2015, I announced 10 additional airports in nine countries that we’ve prioritized for preclearance. In May 2016, CBP announced a new “open season,” running through August 1, for foreign airports to express interest in participating in the next round of preclearance expansion. Twenty-one airports submitted letters of interest. The Department is currently evaluating the submissions and I will make my determination this fall on which airports will participate in the next expansion. I urge Congress to pass

legislation enabling preclearance operations in Canada, by providing legal clarity to CBP officials who are responsible for the day-to-day operation of preclearance facilities there.

For years Congress and others have urged us to develop a system for biometric exit – that is, to take the fingerprints or other biometric data of those who leave the country. CBP has begun testing technologies that can be deployed for this nationwide. With the passage of the FY 2016 Omnibus Appropriations Act, Congress authorized up to \$1 billion in fee increases over a period of 10 years to help pay for the implementation of biometric exit. In April, the Department delivered its Comprehensive Biometric Entry/Exit Plan to Congress, which details CBP’s plan for expanding implementation of a biometric entry/exit system using that funding. I have directed that CBP redouble its efforts to achieve a biometric entry/exit system, and to begin implementing biometric exit, starting at the highest volume airports, in 2018.

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

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

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

Given the nature of the evolving terrorist threat, building bridges to diverse communities is also a homeland security imperative. Well informed families and communities are the best defense against terrorist ideologies. Al Qaeda and ISIL are

targeting vulnerable communities in this country. We must respond. In my view, building bridges to our communities is as important as any of our other homeland security missions.

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

Ensuring that the Nation's CVE efforts are sufficiently resourced has been an integral part of our overall efforts. On July 6, I announced the CVE Grant Program, with \$10 million in available funds provided by Congress in the 2016 Omnibus Appropriations Act. The CVE Grant Program will be administered jointly by OCP and FEMA. This is the first time federal funding at this level will be provided, on a competitive basis, specifically to support local CVE efforts. The funding will be competitively awarded to state, tribal, and local governments, nonprofit organizations, and institutions of higher education to support new and existing community-based efforts to counter violent extremist recruitment and radicalization to violence. The Department issued a notice of funding opportunity on July 6, formally announcing the grant program. Applications were due September 6, and the response has been overwhelming. We received over 200 applications and are currently in the review process.

Finally, I congratulate our personnel for another major accomplishment last week. Led by the U.S. Secret Service, literally thousands of DHS personnel were deployed to New York City for the security of the UN General Assembly. This was a massive undertaking involving over 100 visiting heads of state. This comes in the wake of their successful efforts to lead the protection of the Republican and Democratic National Conventions in Cleveland and Philadelphia July.

Aviation Security

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

Since 2014 we have enhanced security at overseas last-point-of-departure airports, and a number of foreign governments have replicated those enhancements. Security at these last-point-of-departure airports remains a point of focus in light of attacks over the past year, including those in Brussels and Istanbul. By law, TSA is required to assess security at all foreign airports served by U.S. aircraft operators as well as foreign airports serving as last-point-of-departure locations. TSA conducts assessments at over 280 last-point-of-departure airports worldwide.

Last week, I represented the United States at a meeting of the United Nations Security Council, where we adopted the first-ever resolution on aviation security. In recognition of several significant international attacks on civil aviation this past year, the Security Council resolution calls on states to implement effective measures to mitigate threats and urges states to work with ICAO to support the effective implementation of international standards. The adoption of this UNSC resolution is an important step forward in the international community's commitment to aviation security and the advancement of global standards.

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

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

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

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

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

Airlines and airports also assisted in addressing wait times. We appreciate that major airlines and airport operators assigned personnel to certain non-security duties at TSA checkpoints, and provided support in a number of other ways.

Over the summer, the men and women of TSA worked hard to keep passengers moving through security checkpoints, and keep them safe. Their efforts paid off. Between May 25 and August 29 of this year, TSA screened over 200 million passengers and 98% of all passengers waited in line less than 30 minutes. In TSA Pre✓® lanes, 96% of passengers waited less than five minutes. Today, nationwide, the wait time for more than 98% of the traveling public is 30 minutes or less.

But we are not declaring victory. We plan to do more. We are preparing for the upcoming holiday travel season and will continue to work with Congress to ensure TSA has the resources it needs in the coming fiscal years.

Cybersecurity

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

I thank Congress for passing the Cybersecurity Act of 2015. This law is a huge asset to DHS and our cybersecurity mission and we are in the process of implementing it now. While I appreciate the additional authorities granted to us by Congress, I urge you to take further action and establish the Cyber and Infrastructure Protection Agency. The Cyber and Infrastructure Protection Agency would streamline and strengthen existing functions within the Department to ensure we are prepared for the growing cyber threat and the potential for large scale or catastrophic physical consequences as a result of an

attack. With the establishment of the Cyber and Infrastructure Protection Agency, DHS will be best positioned to execute our vital mission.

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

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

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

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

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

I have also directed my team to focus urgently on improving our abilities to protect the Federal Government and private sector. Over the past year, the National Cybersecurity Communications Integration Center, or “NCCIC,” increased its distribution of information, the number of vulnerability assessments conducted, and the number of incident responses.

As required by the law, our NCCIC has built a system to automate the receipt and distribution of cyber threat indicators at real-time speed. We built this in a way that also includes privacy protections.

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

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

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

EINSTEIN 3A is the newest iteration of the system, and has the ability to automatically block potential cyber intrusions on our federal systems. The Cybersecurity Act of 2015 requires federal civilian agencies to apply all available EINSTEIN protections to all information traveling into or out of their networks by the end of this year.

Thus far E3A has actually blocked over a million potential cyber threats, and we are rapidly expanding this capability. About a year ago, E3A covered only about 20% of our federal civilian networks. In the wake of the malicious cyber intrusion at the Office of Personnel Management, in May of last year I directed our cybersecurity team to make at least some aspects of E3A available to all federal departments and agencies by the end of last year. They met that deadline. Now that the system is available to all civilian agencies, 65% of federal personnel are actually protected, including the Office of Personnel Management, and we are working to get all large federal departments and agencies on board by the end of this year. We appreciate your continued support as we work to assist agencies meet their responsibility under the law during the next few months.

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

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

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

In September 2015, DHS awarded a grant to the University of Texas at San Antonio to work with industry to identify a common set of best practices for the development of Information Sharing and Analysis Organizations, or "ISAOs." The

University of Texas at San Antonio recently released the first draft of these best practices. After public comment, they will be released in final form by September 30 and will be updated over the next year.

In recent months we have seen cyber intrusions involving political institutions and personal communications. We have also seen some efforts at cyber intrusions of voter registration data maintained in state election systems. We have confidence in the overall integrity of our electoral systems - it is diverse, subject to local control, and has many checks and balance built in. However, in this environment, we must be vigilant.

I have personally spoken with a number of state Secretaries of State, and DHS stands ready to assist state and local election officials in protecting their systems. In our cybersecurity mission, this is the nature of what we do – offer and provide assistance upon request. We do this for private businesses and other entities across the spectrum of the private and public sectors. DHS assistance is strictly voluntary and does not entail regulation, binding directives, and is not offered to supersede state and local control over the process. Our role is limited to support only.

We have offered the following services to state and election officials to assist in their cybersecurity: remotely conducted cyber hygiene scans on Internet-facing systems, risk and vulnerability assessments done on-site by DHS cybersecurity experts, access to the NCCIC 24x7 incident response center, sharing of relevant information on cyber incidents, sharing of best practices, and access to field-based cybersecurity advisors and protective security advisors. I am pleased that, to date, 18 states have requested our assistance. We will continue to strongly encourage more state and local election officials to do so.

Conclusion

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

I look forward to your questions.