Testimony of Acting Secretary of Homeland Security Elaine C. Duke
"Threats to the Homeland" – Senate Committee on Homeland Security and Government Affairs
September 27, 2017

Chairman Johnson, Ranking Member McCaskill, and distinguished members of the Committee, I would like to thank the Committee for inviting me to testify on the threats facing our great Nation and what we are doing to confront them. First though, I would like to recognize the service of former Secretary John Kelly. While his tenure at the Department of Homeland Security (DHS) ended early, his impact was substantial. General Kelly visibly lifted the morale of the Department, set a new standard for leadership, and—most importantly—established the foundation for historic improvements in our Nation's security. The Department has not missed a beat since his departure, and it is my honor to continue to advance the work he set in motion.

Make no mistake, the threats our country faces are serious. Our enemies and adversaries are persistent. They are working to undermine our people, our interests, and our way of life every day. But whether it is the violent menace posed by international and domestic terrorists or the silent intrusions of cyber adversaries, the American people will not be intimidated or coerced. I am proud that the men and women of DHS are driven to address these challenges, and they are more than equal to the task.

I would like to stress two themes today.

First, we are rethinking homeland security for a new age. We sometimes speak of the "home game" and "away game" in protecting our country, with DHS especially focused on the former. But the line is now blurred. The dangers we face are becoming more dispersed, and threat networks are proliferating across borders. The shifting landscape is challenging our security, so we need to move past traditional defense and non-defense thinking. This is why DHS is overhauling its approach to homeland security. We are bringing together intelligence, operations, interagency engagement, and international action in new ways and changing how we respond to threats to our country.

Second, we are raising the baseline of our security posture—across the board. DHS is looking at everything from traveler screening to information sharing, and we are setting new standards to close security vulnerabilities. Since 9/11, we have spoken too often of the weaknesses in our systems without taking enough decisive action to fix them for the long haul. This Administration aims to change that. At the Department, we are building an action-oriented, results-centric culture. We are pushing our borders outward and pressing foreign partners to enhance their security so that terrorists, criminals, and other threat actors are stopped well before they reach our shores.

Homeland Security in a New Age of Terrorism

Today the magnitude of the threat we face from terrorism is equal to, and in many ways exceeds, the 9/11 period. While we have made it harder for terrorists to execute large-scale attacks, changes in technology have made it is easier for them to plot attacks in general, to radicalize new followers, and to recruit beyond borders. The rising tide of violence we have seen in the West is

clear evidence of this reality. Indeed, acts of terror have become so frequent that we associate them with the names of cities that have been victimized—Paris, San Bernardino, Brussels, Orlando, Istanbul, Nice, Berlin, London, Barcelona, and others. As our government takes the fight to groups such as ISIS and al-Qa'ida in their safe havens, we expect operatives to disperse and focus more heavily on external operations against the United States, our interests, and our allies.

We are seeing an uptick in terrorist activity because the fundamentals of terrorism have evolved. This includes changes in terrorist operations, the profile of individual operatives, and the tactics they use. With regard to operations, terrorist groups historically sought time and space to plot attacks. But now they have become highly networked online, allowing them to spread propaganda worldwide, recruit online, evade detection by plotting in virtual safe havens, and crowd-source attacks. The result is that our interagency partners and allies have tracked a record number of terrorism cases.

Terrorist demographics have also created challenges for our frontline defenders and intelligence professionals. ISIS, al-Qa'ida, and other groups have managed to inspire a wide array of sympathizers across the spectrum. While a preponderance are military-age males, the profile of a terrorist includes young and old, male and female, wealthy and indigent, immigrant and U.S.-born, and living almost anywhere.

The change in terrorist tactics has likewise put strain on our defenses. Global jihadist groups are promoting simple methods, convincing supporters to use guns, knives, vehicles, and other common items to engage in acts of terror. They are also experimenting with other tools—including drones, chemical weapons, and artfully concealed improvised explosive devices—to further spread violence and fear. We have also seen a spider web of threats against the aviation sector, which remains a top target for global jihadist groups. In short, what was once a preference for large-scale attacks is now an "all-of-the-above" approach to terrorism.

The Department is also concerned about violent extremists using the battlefield as a testbed from which they can export terror. We continue to see terrorist groups working to perfect new attack methods in conflict zones that can then be used in external operations. Operatives are packaging this expertise into blueprints that can be shared with followers online and in some cases are providing the material resources needed to conduct attacks. We recently saw this in Australia, when police foiled a major plot to bring down an airliner using a sophisticated explosive device reportedly shipped by an ISIS operative in Turkey.

The primary international terror threat facing the United States is from violent global jihadist groups, who try to radicalize potential operatives within our homeland and seek to send operatives to our country. However, the Department is also focused on the threat of domestic terrorism and the danger posed by ideologically-motivated violent extremists here in the United States. Ideologies like violent racial supremacy and violent anarchist extremism are a danger to our communities, and they must be condemned and countered.

The Department is not standing on the sidelines as these threats spread. And we will not allow pervasive terrorism to become the new normal. We are closely monitoring changes to our

enemies' tactics, and we are working to stay a step ahead of them. This means ensuring that our security posture is dynamic, multi-layered, and difficult to predict. In every respect, DHS has been improving its response. We are doing more to identify terrorists in the first place, changing our programs and practices to adjust to their tactics, and working with our interagency and international partners to find innovative ways to detect and disrupt their plots.

DHS is also working to help our state, local, tribal, territorial and private sector partners —and the public— to be better prepared. We actively share intelligence bulletins and analysis with homeland security stakeholders nationwide to make sure they understand trends related to terrorism and violent extremist activity, know how to guard against nascent attack methods, and are alerted to the potential for violent incidents. For example, in the days prior to the tragic events in Charlottesville, the DHS Office of Intelligence and Analysis partnered with the Virginia Fusion Center to produce and distribute an assessment alerting state and local law enforcement to an increased chance for violence at the upcoming demonstration, which helped enable them to be in place and prepared.

DHS is working closely with private industry and municipalities to help secure public venues and mass gatherings that might be targeted by violent extremists. We have also continued to refine our communications outreach to make sure members of the public report suspicious activity and don't hesitate to do so. Sadly, we have seen many attacks at home and around the world that could have been stopped if someone had spoken up. We want to break that pattern of reluctance.

In many of these areas, we will continue to need Congressional assistance. The President's Fiscal Year 2018 budget calls for a number of counterterrorism improvements that need robust funding. But more must be done to keep up with our enemies. For instance, we lack the authorities needed to counter threats from unmanned aerial systems (UAS). We know that terrorists are using drones to conduct aerial attacks in conflict zones, and already we have seen aspiring terrorists attempt to use them in external operations. Yet DHS and many other departments and agencies do not have the appropriate legal authorities to engage and mitigate these threats in the way we should. Earlier this year, the Administration delivered a government-wide legislative proposal to Congress that would provide additional counter-UAS authorities to DHS and other federal departments and agencies to legally engage and mitigate UAS threats in the National Airspace System. I am eager to share our concerns about UAS in a classified setting, and I urge the Committee to help champion efforts to resolve this and other challenges.

Blocking Threats from Reaching the United States

The Department is undertaking historic efforts to secure our territory. The goal is to prevent national security threat actors, especially terrorists and criminals, from traveling to the United States, while better facilitating lawful trade and travel. The Administration has made it a priority to secure our borders and to provide the American people the security they deserve. We are making it harder for dangerous goods to be flown into our country. And as part of our across-the-board approach to rethinking homeland security, DHS is focusing on uniform improvements to the screening of all categories of U.S.-bound travelers, including visitors, immigrants, and refugees.

Our forward-leaning counterterrorism approach is exemplified by the Department's recent aviation security enhancements. As noted earlier, terrorists continue to plot against multiple aspects of the aviation sector, in some cases using advanced attack methods. Based on carefully evaluated threat intelligence, DHS took action to protect passenger aircraft against serious terror threats. In July, the Department and the Transportation Security Administration (TSA) announced new seen and unseen security measures, representing the most significant aviation security enhancements in many years. Indeed, our ongoing Global Aviation Security Plan is making U.S.-bound flights more secure and will raise the baseline of aviation security worldwide—including additional protections to prevent our enemies from placing threat items in mail or cargo.

Today, terrorists and criminals are exploiting what they see as a borderless world, which is why stepping up our border security must be among the highest national priorities. DHS is actively focused on building out the wall on the Southwest Border and a multi-layered security architecture to keep threats from entering America undetected. We are making measureable progress, and we are cracking down hard on transnational criminal organizations (TCOs), which are bringing drugs, violence, and dangerous goods and individuals across our borders. These organizations have one goal—illicit profit, and they couldn't care less about the enormous human suffering they cause.

TCOs pose a persistent national security threat to the United States. They provide a potential means for transferring weapons of mass destruction (WMD) to terrorists or for facilitating terrorists' entry into the United States. We have already seen migrants with terror connections travel from conflict zones into our Hemisphere, and we are concerned that criminal organizations might assist them in crossing our borders. The shifting travel patterns of these foreign nationals has been cause for concern. TCOs also undermine the stability of countries near our borders, subvert their government institutions, undermine competition in world strategic markets, and threaten interconnected trading, transportation, and transactional systems essential to free markets.

The Administration is fighting back against this threat by using the full force of the Department's authorities and in conjunction with other federal partners. DHS is leading the development of a stronger, fused, whole-of-government approach to border security. Stove-piped agencies cannot prevail against highly-networked adversaries, which is why we are bolstering Joint Task Forces to protect our territory and embedding border security professionals in other relevant departments and agencies. Our Components are coming together on initiatives such as the DHS MS-13 Working Group and the DHS Human Smuggling Cell (HSC). The former, run by U.S. Customs and Border Protection (CBP) and Immigrations and Customs Enforcement (ICE), is identifying gang members previously unknown to law enforcement. The latter is a multi-agency unit staffed by personnel from across the Department that is allowing us to bring together intelligence and operations to go after human smuggling organizations more effectively.

We are also developing comprehensive plans to step up security in the Western Hemisphere and to push the U.S. border outward by shutting down TCOs and smuggling networks. For example, ICE's Biometric Identification Transnational Migration Alert Program (BITMAP) is helping

train and equip foreign counterparts to collect biometric and biographic data on persons of interest and potential threat actors. The data allow us to map illicit pathways, discover emerging TCO trends, and catch known or suspected terrorists and criminals while they are still far from our border.

Beyond border security, DHS is improving almost every stage of the vetting process for U.S.-bound travelers. Front-end investigations of applicants are being modified to more quickly detect individuals with terror ties. Security checks are being brought into the digital age to incorporate social media and other appropriate information. We are gathering additional data from prospective travelers to more effectively validate their identities and determine whether they have connections to terrorists. And DHS is better leveraging unclassified and classified datasets to find previously undetected threats. We have already seen real successes. I cannot get into the details in this setting, but I can share that these enhancements have allowed us to detect and disrupt terror suspects we likely would not have identified otherwise.

Our enhancements span the entire immigration process. For instance, DHS is committed to ICE's Visa Security Program (VSP), which currently assigns special agents to 32 diplomatic posts worldwide to conduct more intensive, up-front scrutiny of visa applications. But security shouldn't stop there. Once an application is approved, we believe there should be recurrent vetting throughout the immigration lifecycle. DHS has been developing Continuous Immigration Vetting (CIV), a real-time systematic process that constantly analyzes visa files against law enforcement and intelligence holdings to identify possible matches to derogatory information. And at our ports of entry, CBP's Tactical Terrorism Response Teams (TTRTs) are connecting dots and finding suspicious individuals we were unaware of previously.

In the medium term, DHS is aiming to streamline how we organize our screening activities. We are examining specific ways to consolidate screening functions, better integrate intelligence data, leverage law enforcement information, and fuse our efforts to protect our country. Both of the witnesses here with me today have been critical partners as we do this and make sure our national vetting efforts are a top priority.

The Department is also pursuing major initiatives to improve international information sharing. We are pressing foreign countries to provide us more data on terrorists and criminals, and we are urging them to use the intelligence our government already provides to catch global jihadists and other threat actors residing in or transiting their territory. DHS is exploring additional measures that could be taken to require foreign governments to take swifter action and how we can better assist them in doing so.

For the first time ever, DHS established a clear baseline for what countries must do to help the United States confidently screen travelers and immigrants from their territory. As required under President Trump's *Executive Order Protecting the Nation from Foreign Terrorist Entry into the United States* (EO 13780), all foreign governments have been notified of the new standards, which include the sharing of terrorist identities, criminal history information, and other data needed to ensure public safety and national security, as well as the condition that countries issue secure biometric passports, report lost and stolen travel documents to INTERPOL, and take other essential actions to prevent identity fraud.

Unfortunately, eight countries failed to meet the new baseline. So I recommended to the President, and he approved, travel restrictions and/or additional scrutiny for nationals of those countries to protect America and pressure those governments to comply with our minimum security standards. Fortunately, most foreign governments met these requirements, and in the process of working with them to understand the new baseline, we managed to negotiate new information sharing arrangements and got commitments to improve travel document security.

Let me be clear: this has nothing to do with race or religion, and our goal is not to block people from visiting the United States. America is proud of its history as a beacon of hope to freedom-loving people from around the world who want to visit our country or become a part of our enduring democratic republic. Rather, the goal is to protect Americans and ensure foreign governments are working with us—and not inhibiting us—from stopping terrorists, criminals, and other national security threat actors from traveling into our communities undetected.

We are also focused on working with our foreign partners to close overseas security gaps that allow dangerous individuals to travel uninhibited. Many countries, for instance, lack the border security policies, traveler screening capabilities, intelligence information sharing practices, and legal tools to effectively stop terrorist travel. DHS is examining the full array of tools at our disposal to incentivize and assist foreign governments in making these improvements so these individuals are caught before they reach our borders.

The Department is not just concerned with threat actors but also threat agents, such as weapons of mass destruction (WMD). Our intelligence professionals have seen renewed terrorist interest in WMD and are aware of concerning developments on these issues, which can be discussed further in an appropriate setting. That is one reason why the Department is eager to establish a focal point for our work to protect Americans against chemical, biological, radiological, and nuclear (CBRN) threats.

The Department's current approach to addressing CBRN matters is inadequate. For nearly a decade, DHS has looked at reorganizing internally to better counter these dangers. We hope to engage with the Committee as we examine how to consolidate our counter-WMD efforts, with the goal of improving our defenses against CBRN threats, creating a focal point for such activities like most other national security departments and agencies, improving strategic direction, instituting business management best practices across the CBRN space, boosting morale, helping with leadership recruitment and retention, and over time reducing waste, overlap, and duplication.

Preventing Terrorist Radicalization and Recruitment in Our Communities

In addition to *counterterrorism*, the Department is rededicating itself to *terrorism prevention*. Americans do not want us to simply stop violent plots, they want us to keep them from materializing in the first place. As part of this effort, we have launched an end-to-end review of all DHS "countering violent extremism," or CVE, programs, projects, and activities. In the coming months we will work to ensure our approach to terrorism prevention is risk-based and

intelligence-driven, focused on effectiveness, and provides appropriate support to those on the frontlines who we rely on to spot signs of terrorist activity.

DHS efforts to combat terrorist recruitment and radicalization fall into four primary lanes.

First, we are prioritizing education and community awareness. Before terrorists have a chance to reach into communities and inspire potential recruits, we are making sure those communities are aware of the threat. This includes extensive outreach to state and locals; awareness briefings; intelligence products regarding threats and trends; training for frontline defenders and civic leaders; and more.

Second, we are focused on counter-recruitment. We know that terrorists will continue to seek new converts through persuasion and propaganda, which is why we must actively push back against solicitations. This includes enabling non-governmental organizations to counter-message terrorist propaganda, leveraging credible voices to dissuade potential recruits, working with social media companies and supporting their efforts to make online platforms more hostile to terrorists, and more.

Last month, I traveled to Silicon Valley to engage with tech companies on this subject, and I am encouraged by the progress they are making, including through the recently announced Global Internet Forum to Counter Terrorism. However, many companies still have a long way to go in shutting down the sprawling network of terrorist accounts and propaganda online. DHS will continue to press companies to quickly identify and remove terrorist content and find new ways to partner with industry. We will also strongly emphasize the importance of counter-messaging—and using credible voices to fight back against the false narrative of terrorist groups. Ultimately, as terrorists crowd-source their violence, the best way to fight back is to turn the crowd against them.

Third, we are emphasizing the importance of early warning. Even with strong community awareness and counter-recruitment, terrorist groups will succeed in reaching at least some susceptible minds. That is why we are working to detect potentially radicalized individuals and terrorist activity earlier. This includes building trust between communities and law enforcement, expanding "See Something, Say Something"-style campaigns, ensuring there are appropriate and confidential means for the public to provide tips regarding suspicious activity, and more.

Finally, DHS is looking at what more can be done to counter terrorist recidivism. It is inevitable that some individuals will be recruited, radicalized, and attempt to engage in terrorist activity. So we want to make sure that once they are caught they do not return to violence. We currently have a number of inmates with terrorism affiliations scheduled for release from U.S. prisons in the next few years, and we need to work with interagency partners to make sure they do not return to violence once released. I look forward to engaging with the Committee further on this subject as we identify effective ways to prevent terrorist recidivism.

This summer the Department announced the award of $10 million in grants to 26 organizations to advance terrorism prevention efforts. These grants will help inform our efforts and illuminate

what works—and what doesn't work—in combating terrorist recruitment and radicalization in our homeland. We look forward to sharing the results with Congress.

I also want to note that although our terrorism prevention activities will be risk-based, they will also be flexible enough to address all forms of extremism. Any ideologically-motivated violence designed to coerce people or their governments should be condemned, prevented, and countered. That is why our approach must be agile so it can mitigate everything from the global jihadist threat to the scourge of violent racial supremacy. It must also engage and not alienate communities targeted by extremists. This means working with people of all races, religions, and creeds as partners in the fight against terror.

Defending America's Digital Frontier

The past year marked a turning point in the cyber domain, putting it in the forefront of public consciousness. We have long faced a relentless assault against our digital networks from a variety of threat actors. But this year, Americans saw advanced persistent threat actors such as hackers, cyber criminals, and nation states, take their attacks to another level. Our adversaries have and continue to develop advanced cyber capabilities. They have deployed them to undermine critical infrastructure, target our livelihoods and innovation, steal our secrets, and threaten our democracy.

Cybersecurity has become a matter of homeland security, and one of the Department's core missions. Significantly, nation-state capabilities are falling into non-state hands. With access to tools that were previously beyond their reach, non-state actors now have the ability to cause widespread disruptions and possibly, destructive attacks. This is redefining homeland security as we know it. And it is affecting everyone, from businesses and governments to individuals who get swept up in data breaches affecting millions of Americans, like what we saw recently with the hack of Equifax.

Many of these threats are novel, as illustrated by the attacks on the Ukrainian power grid in 2015 and 2016, and the use of Internet-connected consumer devices to conduct distributed denial of service attacks. Global cyber incidents, such as the WannaCry ransomware incident in May and the NotPetya malware incident in June, provide recent examples of actors leveraging cyberspace to create widespread disruptive effects and cause economic loss. These incidents exploited known vulnerabilities in software commonly used across the globe.

Prior to these events, DHS was taking key cybersecurity actions through the National Protection Programs Directorate (NPPD), which is responsible for protecting civilian federal networks and collaborating with state, local, tribal, and territorial governments, and the private sector to defend against cyber threats. Through vulnerability scanning, NPPD limited the scope of the potential incident by helping stakeholders identify the vulnerability on their networks so it could be patched before the incident impacted their systems. Recognizing that not all users were able to install patches, DHS shared additional mitigation guidance to assist network defenders. As the incidents unfolded, DHS and our interagency partners led the Federal Government's incident response efforts in accordance with agencies' responsibilities set forth in Presidential Policy Directive 41, including providing situational awareness, information sharing, malware analysis,

and technical assistance to affected entities.

Historically, cyber actors have strategically targeted the energy sector with various goals ranging from cyber espionage to developing the ability to disrupt energy systems in the event of a hostile conflict. In one recent campaign, advanced persistent threat actors targeted the cyber infrastructure of entities within the energy, nuclear, critical manufacturing, and other critical infrastructure sectors. In response, DHS, the Federal Bureau of Investigation, and the U.S. Department of Energy shared information to assists network defenders identify and reduce exposure to malicious activity.

In the face of these digital threats, it is a DHS priority to work with Congress on legislation that would focus our cybersecurity and critical infrastructure mission at NPPD. We are pursuing changes that would streamline and elevate NPPD's mission. Through transition from a headquarters component to a DHS operating component, with better structure, the DHS Cyber and Infrastructure Security Agency would be better position to drive our cybersecurity mission.

We are also endeavoring to enhance cyber-threat information sharing across the globe to stop attacks before they start—and to help Americans quickly recover. We work closely with technology providers, information-sharing and analysis centers, sector coordinating councils, and critical infrastructure owners and operators to brief them on cyber threats and provide mitigation recommendations, and our hunt and incident response teams provide expert intrusions analysis and mitigation guidance to stakeholders who request assistance in advance of and in response to a cyber incident.

In all its cybersecurity efforts, DHS draws upon its experience in emergency management and counterterrorism by taking a broad risk management approach. DHS considers cybersecurity risk within the landscape of overall threats to the Nation and an assessment of the likely consequences of cyber incidents which may or may not result in physical impacts.
To increase the security and resilience of nonfederal critical infrastructure, DHS leverages information and expertise gained from the federal protective mission. DHS makes technical capabilities and programs available to nonfederal entities and provides cybersecurity information and recommendations to, and partners closely with, a variety of private sector, State, local, tribal, and territorial, and international stakeholders. This information and technical assistance allows our stakeholders to make informed risk management decisions and to improve their cybersecurity.

At the same time, the U.S. Secret Service and HSI work closely with other law enforcement partners to aggressively investigate, disrupt, and dismantle criminal actors and organizations using cyberspace to carry out their illicit activities. The efforts of the network protection and law enforcement experts must be increasingly coordinated within the Department and with other agencies and non-federal entities. Information about tactics and trends obtained through law enforcement investigations inform other network protection efforts, including those through the National Cybersecurity and Communications Integration Center (NCCIC), to raise the defensive capabilities of the Nation. And the efforts of network protectors can identify trends, practices, and potentially new victims to shape law enforcement investigations. Together these efforts are an important part of an overall national approach to deterrence by denying malicious actors

access to critical U.S. targets, increasing resilience of networks, and by identifying and punishing those who try to use cyberspace for illicit purposes.

Bringing together its network protection, law enforcement, risk mitigation, and emergency management expertise, DHS plays a lead role in the federal government's response to cyber incidents. Such incidents can result from malicious activity as well as natural or accidental causes. The NCCIC and DHS law enforcement components provide assistance to impacted entities. The Office of Intelligence and Analysis (I&A) and component intelligence offices play a supporting role by providing relevant intelligence support to DHS components from across the intelligence community. Sector specific agencies provide unique expertise and insights to response activities and help DHS ensure that lessons learned from incidents are incorporated into efforts to protect critical information systems. DHS works closely with sector specific agencies, the Department of Defense, the Department of Justice and the FBI before, during, and after incidents.

In support of these operational efforts, DHS also works to strengthen the overall security and reliability of the cyber ecosystem. Because cyberspace is inherently global, DHS collaborates with the international community to exchange and advocate for best practices and promote the development and adoption of normative behavior to increase security and reliability. Additionally, in order to build up capacity for tackling emerging challenges and supporting the overall cybersecurity mission, DHS drives research, development, and technology transfer efforts and works with industry stakeholders to make the Internet and new technologies, like the Internet of Things, more secure. Finally, DHS prioritizes the expansion of the human resource programs to recruit, hire, develop, and retain personnel with strong cybersecurity skillsets.

Conclusion

I want to emphasize that we are overhauling homeland security to cope with changes in the threat landscape. Our leadership team is breaking down legacy bureaucratic barriers to make DHS operate more efficiently and effectively to counter threats to our nation. We are ramping up unity of effort within the department and tight collaboration with law enforcement, the intelligence community, and our allies. And we are looking at ways to further integrate intelligence and operations so that our actions are driven by timely information and that we respond quickly to new dangers.

As we continue this overhaul, it is clear that the authorities, structures, and accountability measures developed for DHS over 15 years ago are no longer sufficient. We simply cannot keep the United States and its citizens secure with authorities drafted before smartphones and social media, as such technology has further blurred the line between the "home game" and "away game."

On July 20, 2017, the House passed comprehensive legislation reauthorizing the Department of Homeland Security. This legislation would be the Department's first ever reauthorization – and for certain parts of the Department, it would be their first actual authorization. H.R. 2825 reflects the Department's importance in our national security efforts, and it solidifies our mission to protect our nation now and into the future. It empowers the men and women who protect our

nation to better execute their mission. It authorizes replacement and modernization of outdated Coast Guard vessels, with an eye toward making the most of taxpayer dollars. It allows us to study disaster preparedness and response, so we can find ways to help communities recover more quickly and efficiently. It establishes standards for first responders to get the training and equipment they need to counter the terrorist threats of today. And it improves the Departments information sharing capabilities, so our state, local, tribal, and territorial partners can stay up-to-date on the threats facing our communities, in both the cyber and the physical world.

There is no more important mission – no duty more sacred – than protecting the people of the United States. Passing legislation to reauthorize DHS is an opportunity for Congress to show its commitment to that mission and to the men and women charged with executing that mission every day. I strongly encourage this Committee and the Senate to take up and pass legislation reauthorizing DHS as quickly as possible. DHS stands ready to assist in any way that we can.

Thank you for the opportunity to appear before you today and for your continued support of DHS. I am committed to working with this Committee to forge a strong and productive relationship as we work to achieve the shared objective of securing our homeland.