TESTIMONY OF ACTING SECRETARY OF HOMELAND SECURITY ELAINE C. DUKE

"World Wide Threats: Keeping America Secure in the New Age of Terror"

THE HOUSE COMMITTEE ON HOMELAND SECURITY

November 30, 2017

Chairman McCaul, Ranking Member Thompson, and distinguished members of the Committee, I would like to thank you 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 until such time as the Senate votes to confirm the President's nominee, Kirstjen Nielsen.

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. 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 three 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 border security strategies and pressing foreign partners to enhance their security so that terrorists, criminals, and other threat actors are stopped well before they reach our shores.

Third, this unprecedented hurricane season has truly tested us as a nation and tested many of our assumptions about what works in disaster response and recovery. While each year the hurricane season officially comes to an end on November 30, the lessons that we are learning from the response and recovery operations that we are performing this year, under the most difficult circumstances possible, will transform the field of emergency management forever.

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 easier for adversaries to plot attacks in general, to radicalize new followers, and to recruit beyond borders. The problem is compounded by the use of simple, "do-it-yourself" terrorist tactics.

The rising tide of violence we have seen in the West is clear evidence of the serious threat. Acts of terrorism and mass violence against soft targets 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 most recently in New York City on Halloween. As our government takes the fight to groups such as ISIS and al-Qa'ida, 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 young men, they can be young or old, male or female, wealthy or indigent, immigrant or 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 terrorism. At the same time, they are 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. This is particularly exacerbated by the increased emphasis on so-called soft targets. Locations, venues, or events associated with public gatherings are increasingly appealing targets for terrorists and other violent criminals because of their accessibility and the potential to inflict significant physical, psychological, and economic damage.

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. In some cases, terrorists are even 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 overseas.

The primary international terror threat facing the United States is from violent global jihadist groups, who try to radicalize potential followers within our homeland and who 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. 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.

DHS is working closely with private industry and municipalities to help secure public venues and mass gatherings that might be targeted by terrorism and violent extremist activity. We have also continued to refine our 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. In some cases, DHS and other departments and agencies lack certain legal authorities to engage and mitigate the emerging dangers we are seeing. For example, we lack the authorities needed to counter threats from unmanned aircraft 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 attacks outside the conflict zone.

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 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 enter our country. And as part of our across-the-board approach to rethinking homeland security, DHS is improving 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 this year to protect passenger aircraft against serious terror threats. This summer, we 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 dangerous 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 aliens with terror connections travel from conflict zones into our Hemisphere, and we are concerned that TCOs might assist them in crossing our borders. 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 Department is fighting back against this threat by using its full authorities and working in concert 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 working together on initiatives such as the DHS MS-13 Working Group and the DHS Human Smuggling Cell. The former, run by U.S. Customs and Border Protection (CBP) and U.S. Immigration 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 threats. 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, including through ICE's Visa Security Program. Security checks are being brought into the digital age with measures like continuous immigration vetting, a real-time, systematic process that constantly analyzes visa files against law enforcement and intelligence holdings to identify possible matches to derogatory information. At the same time, we are gathering additional data from prospective travelers to more effectively validate their identities and determine whether they pose a risk to our country.

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, suffice to say that these enhancements have allowed us to detect and disrupt terror suspects we likely would not have identified otherwise. And at our ports of entry, CBP's Tactical Terrorism Response Teams are connecting dots and finding suspicious individuals we might also have otherwise slipped through the cracks.

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 Administration is also pursuing major initiatives to improve international information sharing. Working with the State Department and interagency, we are pressing foreign countries to provide us more information on terrorists and criminals, and we are urging them to use the

information 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.

DHS assessed whether countries met the new standards, in consultation with the Department of State and the Department of Justice. Countries that failed to do so were recommended to the President for travel restrictions or other lawful limitations, which he imposed through a Presidential proclamation in October. Most foreign governments have met these minimum standards or are on the path to doing so. For those that the President has designated for restrictions, we have indicated that we will consider relief, but first they must comply with these reasonable, baseline requirements.

This has nothing to do with race or religion, and our goal is not to block people from visiting the United States. America has a proud 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.

I commend the House Homeland Security Committee for examining these matters as part of its Task Force on Denying Terrorists Entry into the United States. As you prepare your final recommendations, the Department stands ready to work with you to implement them.

DHS 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 setting up a focal point within DHS for our work to protect Americans against chemical, biological, radiological, and nuclear (CBRN) threats.

The Department's previous approach to addressing CBRN threats was inadequate and our organization for this mission has been fragmented. For nearly a decade, DHS considered internally reorganizing to ensure our Department's counter-WMD efforts were unified. Given the growing threats and the need to enhance DHS's ability to help respond, I notified Congress of our intent to create a Countering Weapons of Mass Destruction (CWMD) Office using the Secretary's re-organization authority under Section 872 of the Homeland Security Act. We are exercising this authority for a limited, internal re-organization to achieve unity of command, and we intend to work collaboratively with Congress formalize this office and ensure it is postured appropriately to confront the threat. We look forward to continuing to engage with this Committee as we examine how to consolidate our counter-WMD efforts, with the goal of ensuring our Nation is safer than ever before.

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 states and localities, 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 followers through persuasion and propaganda, which is why we must support efforts to actively push back against such solicitations. This includes continuing to encourage 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 met with the Interior Ministries of the G7 counties in Italy and some of the largest technology companies and discussed the next steps the companies plan to take in the effort to prevent their platforms from being misused by terrorists, including better identifying online terrorist propaganda and shutting down terrorist accounts. The meeting emphasized the importance of working together with our foreign partners while we continue to engage industry on this important issue. The U.S. Government has already made progress by supporting the companies' efforts—including the establishment of the Global Internet Forum to Counter

Terrorism—to identify terrorist content so they can voluntarily remove content that violates their terms of service as soon as it is discovered.

Many companies, however, still have substantial challenges in quickly identifying and addressing the volume of terrorist accounts and propaganda online. DHS, along with interagency partners, will continue sharing information and educating private sector partners on how to more quickly identify and address terrorist content. 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 "If You 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. A number of inmates with terrorism affiliations are scheduled for release from U.S. prisons in the next few years. We need to work with the Department of Justice and its Bureau of Prisons, and other 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 terrorism. Any ideologically-motivated violence which is designed to coerce people or their governments should be condemned, prevented, and countered. That is why our approach must be agile so it can help mitigate everything from the global jihadist threat to the scourge of violent racial supremacy. It must also engage and not alienate communities targeted by these fanatics. This means working with people of all races, religions, and creeds as partners in the fight against terrorism.

Securing Soft Targets

As I mentioned earlier, terrorists and other violent criminals are placing significant emphasis on attacking soft targets. We have seen this with recent tragedies in Nevada, New York, and Texas. Although the Department has previously focused on enhancing the security of such facilities, it

has recently placed further emphasis on assisting the critical infrastructure community to secure these vulnerable facilities. For example, the National Protection and Programs Directorate (NPPD) will make the Department the national leader on technology, standards, and best practices relating to soft target security. The intent of the effort is to:

- Demonstrably reduce the risk of a successful attack on soft targets;
- Ensure the Department has the capability to support visible efforts to enhance soft target security in order to safeguard the American people;
- Develop a center of gravity for Department-wide resources available to support the critical infrastructure community in securing soft targets;
- Promote a dynamic process to identify and address soft target security gaps based on threats and incidents.

Efforts such as the Hometown Security Initiative, in conjunction with our programs that provide training and informational resources focused on active shooter preparedness, play a key role in preparing facilities and their employees to proactively think about the role they play in the safety and security of their businesses and communities.

In addition, the S&T SAFETY Act Program provides important legal liability protections of qualified anti-terrorism technologies in order to encourage the development and deployment of effective products and services that enhance security. The Program is intended to provide critical incentives for the development and deployment of anti-terrorism technologies by providing liability protections for "qualified anti-terrorism technologies."

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 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 national security, and one of the Department's core missions. 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.

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. Other recent global cyber incidents, such as the *WannaCry* ransomware incident in May and the *NotPetya* malware incident in June 2017, exploited known vulnerabilities in software commonly used across the globe to create widespread disruptive effects and cause economic loss.

DHS defends from these attacks and provides tools to mitigate ongoing incidents through the National Protection and Programs Directorate (NPPD), which is in addition to protecting civilian federal networks collaborates with state, local, tribal, and territorial governments, and the private sector to defend against cyber threats. Through vulnerability scanning, NPPD limited the scope of potential incidents 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.

Cyber actors continue to target 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 assist 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 ICE Homeland Security Investigations work closely with FBI, as well as 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 NPPD, 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. NPPD and DHS law enforcement components provide assistance to impacted entities. 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. As 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 its human resource programs to recruit, hire, develop, and retain personnel with strong cybersecurity skillsets.

2017 Hurricane Season

To say the 2017 hurricane season has been historic is an understatement. To date, we've had four hurricanes make landfall this season, three of which have been major hurricanes (Harvey, Irma, and Maria). Prior to Harvey making landfall on August 25, 2017, FEMA was supporting 28 presidentially-declared disasters. Since Hurricane Harvey made landfall in Texas, the President has granted 14 Major Disaster declarations and 14 Emergency Declarations, while FEMA has authorized 25 Fire Management Assistance Grant declarations. Hurricane Irma was unique not only because it struck both the U.S. Virgin Islands and Puerto Rico, but also because it struck the entire State of Florida. Hurricane Maria, following in quick succession, then struck the U.S. Virgin Islands and Puerto Rico, more than 1,000 nautical miles from the mainland United States, devastating an area with already fragile infrastructure and facing challenging

economic circumstances. In a span of 25 days, DHS, FEMA, and our partners deployed tens of thousands of personnel across 270,000 square miles in three different Regions.

The impacts of these events are substantial. Roughly 25.8 million people were affected by these three storms – eight percent of the entire U.S. population. As of November 13, 2017, more than four and a half million survivors registered for FEMA assistance, which is a greater number than Hurricanes Katrina, Rita, Wilma and Sandy combined. FEMA's Individual and Households Program (IHP) has thus far approved almost $2.5 billion in disaster assistance to respond to the three hurricanes, a number we expect to continue to grow. As of mid-November, National Flood Insurance Program (NFIP) policyholders filed approximately 121,000 claims, and the NFIP has paid over $5 billion to them.

DHS and FEMA alone cannot deliver assistance to this vast number of survivors. Unity of effort is required for disaster response and recovery on any scale, but especially during this historic season. When emergency managers call for unity of effort, we mean that all levels of government, non-profit organizations, private sector businesses, and survivors must work together – each drawing upon their unique skills and capabilities – to meet the needs of disaster survivors.

For our part on the Federal level, FEMA called upon the vast majority of their workforce, while I engaged over 3,800 other Federal employees through the DHS "Surge Capacity Force." This is significant. FEMA employees come to FEMA knowing they will be deployed into disaster areas, work in austere conditions, and assist survivors. However, when personnel from other Federal agencies volunteer for the Surge Capacity Force, they volunteer to leave their jobs and families, receive just-in-time training, and work in an environment that is completely unfamiliar and outside of their normal job responsibilities. I am incredibly grateful to my colleagues from across the Federal government for supporting this important initiative, and for allowing their hardworking and dedicated personnel to support disaster survivors who have been impacted by these historic events. Over 22,300 members of the Federal workforce were deployed to Texas, Florida, the U.S. Virgin Islands, and Puerto Rico. This includes 13,892 staff from various offices of the Department of Defense, including the military services. We could not do this without them.

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.

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.