Homeland Security

Written testimony of Department of Homeland Security Secretary Janet Napolitano for a Senate Committee on the Judiciary hearing titled "The Oversight of the Department of Homeland Security"

Release Date: April 25, 2012

226 Dirksen

Introduction

Chairman Leahy, Ranking Member Grassley, and Members of the Committee:

I am pleased to join you today, and I thank the Committee for your strong support for the Department of Homeland Security (DHS) over the past three years and, indeed, since the Department's founding more than nine years ago. I look forward to continuing to work with you to protect the American people as we work to advance our many shared goals.

Today, ten years after the September 11th attacks, America is stronger and more secure, thanks to the support of the Congress, the work of the men and women of DHS, and our federal, state, local, tribal, and territorial partners across the homeland security enterprise.

More than 230,000 DHS employees ensure the safety and security of the American people every day, in jobs that range from law enforcement officers and agents to disaster response coordinators, from those who make sure our waterways stay open to commerce to those who make sure our skies remain safe. The men and women of DHS are committed to our mission, and I thank every one of them for their service.

As I have said many times, homeland security begins with hometown security. As part of our commitment to strengthening hometown security, we have worked to get information, tools, and resources out of Washington, D.C., and into the hands of state, local, tribal, and territorial officials and first responders.

This has led to significant advances. We have made great progress in improving our domestic capabilities to detect and prevent terrorist attacks against our people, our communities, and our critical infrastructure. We have increased our ability to analyze and distribute threat information at all levels. We have invested in training for local law enforcement and first responders of all types in order to increase expertise and capacity at the local level. And we have supported and sustained preparedness and response capabilities across the country through approximately $35 billion in homeland security grants since 2002.

We work with a vast array of partners, from local law enforcement, the private sector, and community leaders across the country, all of whom understand our shared responsibility for public safety and are committed to doing their part to help keep America safe.

To continue to build on these efforts, the Administration has proposed a new homeland security grants program in Fiscal Year 2013 designed to develop, sustain, and leverage core capabilities across the country in support of national preparedness, prevention, and response. The Fiscal Year 2013 National Preparedness Grant Program (NPGP) will help create a robust national preparedness capacity based on cross-jurisdictional and readily deployable state, local, tribal, and territorial assets. Using a competitive, risk-based model, the NPGP will use a comprehensive process for identifying and prioritizing deployable capabilities, limit periods of performance to put funding to work quickly, and require grantees to regularly report progress in the acquisition and development of these capabilities.

Our experience over the past several years also has made us smarter about the terrorist threats we face and how best to deal with them. We have learned that an engaged, vigilant public is essential to efforts to prevent acts of terrorism, which is why

we have continued to expand the "If You See Something, Say Something™" campaign nationally. We also continue to expand our risk-based, intelligence-driven security efforts. By sharing and leveraging information, we can make informed decisions about how to best mitigate risk, and the more we know, the better we become at providing security that is seamless and efficient. We also free up more time and resources, giving us the ability to focus those resources on those threats or individuals that we know less about.

Additionally, over the past several years, we have deployed unprecedented levels of personnel, technology, and resources to protect our nation's borders. These efforts have achieved significant results, including historic decreases in illegal immigration as measured by total apprehensions, and increases in seizures of illegal drugs, weapons, cash, and contraband.

We also have focused on smart and effective enforcement of immigration laws while streamlining and facilitating the legal immigration process. Our enforcement resources prioritize the identification and removal of criminal aliens and repeat immigration law violators, recent border entrants, and immigration fugitives. We also are identifying and sanctioning employers who knowingly hire workers, not authorized to work in the United States, and—by doing so—undercut employers who follow the rules.

The Department also continues to lead the federal government's efforts to secure civilian government computer systems and works with industry and state, local, tribal, and territorial governments to secure critical infrastructure and information systems. We are deploying the latest tools across the federal government to protect critical civilian systems, while sharing timely and actionable security information with public and private sector partners to help them protect their own operations. Together with our public and private sector partners, we are protecting the systems and networks that support the financial services industry, the electric power industry, and the telecommunications industry, to name a few.

Strengthening homeland security also includes a significant international dimension. To most effectively carry out our core missions – including preventing terrorism, securing our borders and enforcing immigration laws, and protecting cyberspace – we partner with countries around the world. This work ranges from strengthening cargo, aviation, and supply chain security to joint investigations, information sharing, and science and technology cooperation. Through collaborations with other federal agencies and our foreign counterparts, we not only enhance our ability to prevent terrorism and transnational crime; we also leverage the resources of our international partners to more efficiently and cost-effectively secure global trade and travel, in order to ensure that dangerous people and goods do not enter our country.

In my time today, I would like to provide an update on the key areas of the DHS mission that fall within the Committee's jurisdiction, our priorities for the coming year, and our vision for working with the Congress to build on the substantial progress we have achieved to date and must continue to sustain in the months and years ahead.

Preventing Terrorism and Enhancing Security

While the United States has made significant progress, threats from terrorism—including, but not limited to al-Qaeda and al-Qaeda affiliated groups—persist and continually evolve, and the demands on DHS continue to grow. Today's threats are not limited to any one individual, group or ideology and are not defined or contained by international borders. Terrorist tactics can be as simple as a homemade bomb and as sophisticated as a biological threat or a coordinated cyber attack.

DHS and our partners at the federal, state, tribal, and local levels have had success in thwarting numerous terrorist plots, including the attempted bombings of the New York City subway and Times Square, foiled attacks against air cargo, and other attempts across the country. Nonetheless, recent attacks overseas, including the attacks in Toulouse, France last month and the continued threat of homegrown terrorism in the United States, demonstrate how we must constantly remain vigilant and prepared.

To address these evolving threats, DHS employs risk-based, intelligence-driven operations to prevent terrorist attacks. Through a multi-layered detection system focusing on enhanced targeting and information sharing, we work to interdict threats and dangerous people at the earliest point possible. We also work closely with federal, state, and local law enforcement partners on a wide range of critical homeland security issues in order to provide those on the frontlines with the information and tools they need to address threats in their communities.

Sharing Information, Expanding Training, and Raising Public Awareness

The effective sharing of information in a way that is timely, actionable whenever possible, and adds value to the homeland security enterprise is essential to protecting the United States. As part of our approach, we have changed the way DHS provides information to our partners by replacing the old color-coded alert system with the new National Terrorism Advisory System, or NTAS, which provides timely, detailed information about credible terrorist threats and recommended security

measures.

We also have continued to enhance our analytic capability through the 77 designated fusion centers, resulting in unprecedented information sharing capabilities at the state and local levels. DHS has supported the development of fusion centers through deployed personnel, training, technical assistance, exercise support, security clearances, connectivity to federal systems, technology, and grant funding.

We currently have more than 90 DHS intelligence officers deployed to fusion centers, working side by side with their federal, state, and local counterparts. Sixty-three fusion centers can now receive classified and unclassified threat information through the Homeland Secure Data Network, or HSDN.

We are also working to ensure that every fusion center supported by DHS maintains a set of core capabilities that includes the ability to assess local implications of national intelligence, share information with federal authorities so we can identify emerging national threats, and ensure the protection of civil rights, civil liberties and privacy.

Specifically, we are encouraging fusion centers to develop and strengthen their grassroots analytic capabilities so that national intelligence can be placed into local context, and the domestic threat picture can be enhanced based on an understanding of the threats in local communities. We are partnering with fusion centers to establish more rigorous analytic processes and analytic production plans, increasing opportunities for training and professional development for state and local analysts, and encouraging the development of joint products among fusion centers and federal partners.

Over the past three years, we also have transformed how we train our nation's frontline officers regarding suspicious activities, through the Nationwide Suspicious Activity Reporting Initiative. This initiative, which we conduct in partnership with the Department of Justice, is an administration effort to train state and local law enforcement to recognize behaviors and indicators related to terrorism and terrorism-related crime; standardize how those observations are documented and analyzed; and ensure the sharing of those reports with the Federal Bureau of Investigation-led Joint Terrorism Task Forces (JTTFs) for further investigation.

More than 213,000 law enforcement officers have now received training under this initiative, and more are getting trained every week. The training was created in collaboration with numerous law enforcement agencies, and with privacy, civil rights and civil liberties officials. DHS also has expanded the Nationwide Suspicious Activity Reporting Initiative to include our nation's 18 critical infrastructure sectors. Infrastructure owners and operators from the 18 sectors are now contributing information, vetted by law enforcement through the same screening process otherwise used to provide information to the JTTFs.

Because an engaged and vigilant public is vital to our efforts to protect our communities from violence, including that resulting from terrorism, we also have continued our nationwide expansion of the "If You See Something, Say Something™" public awareness campaign. This campaign encourages Americans to contact law enforcement if they see something suspicious or potentially dangerous. To date, we have expanded the campaign to federal buildings, transit systems, major sports and entertainment venues, some of our nation's largest retailers, as well as many law enforcement partners. We will continue to expand the campaign even further this year.

Countering Violent Extremism

At DHS, we believe that local authorities and community members are often best able to identify individuals or groups residing within their communities exhibiting dangerous behaviors—and intervene—before they commit an act of violence. Countering violent extremism (CVE) is a shared responsibility, and DHS continues to work with a broad range of partners to gain a better understanding of the behaviors, tactics, and other indicators that could point to terrorist activity, and the best ways to mitigate or prevent that activity.

The Department's efforts to counter violent extremism are three-fold. We are working to better understand the phenomenon of violent extremism, and assess the threat it poses to the Nation as a whole, and within specific communities. We are bolstering efforts to address the dynamics of violent extremism and strengthen relationships with those communities targeted for recruitment by violent extremists. We are also expanding support for information-driven, community-oriented policing efforts that have proven effective in preventing violent crime across the nation for decades.

As part of this approach, and consistent with the Administration's strategy released in August 2011and the related Strategic Implementation Plan released in December 2011, we are implementing a CVE curriculum for state and local law enforcement that is focused on community-oriented policing, which will help frontline personnel identify activities that are potential indicators of potential terrorist activity and violence. We piloted the curriculum in San Diego in January 2012, and we are working with the International Association of Chiefs of Police (IACP) to implement the curriculum in law enforcement academies nationwide.

We are also developing a similar curriculum with the Federal Law Enforcement Training Center (FLETC) for federal law enforcement officers.

With local communities and the Department of Justice, we have published guidance on best practices for community partnerships to prevent and mitigate homegrown threats. And we have issued, and continue to release, unclassified case studies that examine recent incidents involving terrorism so all of us can better understand the potential warning signs of violent extremism.

Protecting Our Aviation System

We have continued to strengthen protection of our aviation sector through a layered detection system focusing on risk-based screening, enhanced targeting, and information-sharing efforts to interdict threats and dangerous people at the earliest point possible.

The Department is focused on measures to evolve aviation security from a "one size fits all" approach for passenger screening to a risk-based approach to security. In doing so, TSA utilizes a range of measures, both seen and unseen. Our nation's aviation sector continues to be a high threat terrorist target. There is currently no silver bullet; however we utilize a layered approach that seeks to both protect the aviation system and expedite passenger travel.

The Transportation Security Administration (TSA) has deployed approximately 650 Advanced Imaging Technology (AIT) units to airports across the United States to assist our Transportation Security Officers in safely screening passengers for metallic and non-metallic threats. TSA has now installed new software on all millimeter wave AIT machines to enhance privacy by eliminating passenger-specific images and TSA is working closely with the vendor to deploy this capability to backscatter units as quickly as possible. TSA also continues to deploy Explosives Detection Systems to airports to efficiently screen baggage for explosives while reducing the number of physical bag searches

Additionally, TSA has added more canine teams, which serve as an important layer of security to complement passenger checkpoint screening at airports, assist in air cargo screening, and enhance security in the mass transit environment. And through Secure Flight, TSA is now pre-screening 100 percent of all travelers flying within, to, or from the United States against terrorist watchlists before passengers receive their boarding passes.

As we have taken these actions to strengthen security, we also have focused on expediting trade and travel for the millions of people who rely on our aviation system every day. One key way we have done this is through expansion of trusted traveler programs.

For instance, the Global Entry program, which is managed by U.S. Customs and Border Protection (CBP), is allowing us to expedite entry into the United States for pre-approved, low-risk air travelers. More than one million passengers have already joined Global Entry, and we are expanding the program as part of the Administration's efforts to foster travel and tourism.

Global Entry participants are also eligible for TSA Pre✓™. TSA Pre✓™ is a domestic expedited traveler initiative that enhances security by allowing us to focus on passengers we know less about and those who are considered high-risk, while providing expedited screening for travelers who volunteer information about themselves prior to flying. Efforts like TSA Pre✓™ represent an important evolution in the way we handle airline security, as we shift away from the one-size-fits-all model of passenger screening to one that is risk-based.

In our increasingly interconnected world, we also work beyond our own airports to protect both national and economic security through partnerships with international allies and other Federal agencies, and enhanced targeting and information-sharing efforts to interdict threats and dangerous people and cargo at the earliest point possible.

For example, through the Pre-Departure Targeting Program and Immigration Advisory Program and enhanced in-bound targeting operations, CBP has improved its ability to identify high-risk travelers who are likely to be inadmissible into the United States and make recommendations to commercial carriers to deny boarding before a plane departs.

Through the Visa Security Program and with Department of State concurrence, U.S. Immigration and Customs Enforcement (ICE) has deployed trained special agents overseas to high-risk visa activity posts to identify potential terrorist and criminal threats before they reach the United States.

Through preclearance agreements, CBP is also inspecting passengers internationally prior to takeoff through the same process a traveler would undergo upon arrival at a U.S. port of entry, allowing us to extend our borders outward while facilitating a more efficient passenger experience.

Our continued use, analysis, and sharing of Passenger Name Record (PNR) data has allowed us to better identify passengers we should pay more attention to before they arrive at the airport they are departing from overseas. In December 2011, we signed a new agreement with the European Union to continue the transfer of PNR data, an important milestone in our collective efforts to protect the international aviation system from terrorism and other threats.

Visa Waiver Program

With our partners overseas, we also have acted to strengthen the Visa Waiver Program (VWP), which allows eligible nationals of 36 countries to travel to the United States without a visa and remain in our country for up to 90 days for tourist or business purposes. Since its inception in the mid-1980s, the VWP has become an essential tool for increasing security standards, advancing information sharing, strengthening international relationships, and promoting legitimate travel to the United States.

Over the last several years, DHS has focused on bringing VWP countries into compliance with information sharing agreement requirements of The Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Act), Pub. L. No.110-53. As of January 2012, all VWP countries have completed an exchange of diplomatic notes or an equivalent mechanism for the requirement to enter into an agreement to share information on lost and stolen passports with the United States through INTERPOL or other designated means.

DHS also has signed Preventing and Combating Serious Crime (PCSC) agreements with 22 VWP countries which facilitate the sharing of information about terrorists and criminals. Negotiations on four additional PCSC Agreements with VWP countries have been completed, and we have an equivalent agreement already in force with the United Kingdom.

Additionally, DHS developed the Electronic System for Travel Authorization (ESTA) as a proactive online system to determine whether an individual is eligible to travel to the United States under the VWP, and whether such travel poses any law enforcement or national security risks. The system was created in response to a requirement in the 9/11 Act, which mandated that all citizens of VWP eligible countries who plan to travel to the United States under the VWP, must obtain an electronic travel authorization prior to boarding a U.S.-bound commercial flight or cruise ship.

Overstays and Exit Capabilities

Over the past year, we also have worked to better detect and deter those who overstay their lawful period of admission. The ability to identify and sanction overstays derives from the ability to determine who has arrived and departed from the United States. By matching arrival and departure records and using additional data collected by DHS, we can better determine who has overstayed their lawful period of admission.

In May 2011, DHS began a coordinated effort to vet all potential overstay records against Intelligence Community and DHS holdings for national security and public safety concerns. In total, using those parameters, we reviewed the backlog of 1.6 million overstay leads within the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) program and referred leads based on national security and public safety priorities to ICE for further investigation.

A beneficial by-product of this vetting effort has been the identification of efficiencies gained through automation, as well as other enhancements. Through a new automated system, we will be able to enhance automated matching, eliminate gaps in travel history, and aggregate information from multiple systems.

In October 2011, I proposed a strategy to Congress to utilize DHS funds to implement an automated vetting and enhanced biographic exit capability. This strategy will allow the Department to significantly enhance our existing capability to identify and target for enforcement action those who have overstayed their authorized period of admission, and who represent a public safety and/or national security threat by incorporating data contained within law enforcement, military, and intelligence repositories.

This strategy also will enhance our ability to identify individual overstays and determine overstay percentages by country; provide the State Department with information to support visa revocation, prohibit Visa Waiver Program travel, and place "lookouts" for individuals, in accordance with existing Federal laws; establish greater efficiencies to our Visa Security Program; and enhance the core components of an entry-exit and overstay program.

I have directed the Science and Technology Directorate (S&T) to establish criteria and promote research for emerging technologies that would provide the ability to capture biometrics at a significantly lower operational cost. S&T is working closely with the National Institute of Standards and Technology (NIST) on this initiative, and S&T expects to have a report shortly detailing potential next steps and a road map for the next several years concerning potential capabilities for a future biometric air exit system, including how anticipated technology enhancements can fit within the DHS operational environment.

Following this analysis, we anticipate beginning controlled and scenario-based lab testing within the year and operational testing in less than three years. Overall, if the evaluated approach is determined to be cost effective, the Department will be able to consider deployment of a biometric exit capability within four years.

In addition, we are working toward a system to create an exit program on the United States northern land border to facilitate the exchange of U.S. and Canadian entry records, so that an entry to one country becomes an exit from another.

We support carefully managed expansion of the VWP to countries that meet the statutory requirements, and are willing and able to enter into a close security relationship with the United States. To this end, we support current bi-partisan efforts by the Congress to expand VWP participation and also to promote international travel and tourism to the United States while maintaining our strong commitment to security.

Protecting Surface Transportation

Beyond aviation, we have worked with transportation sector entities and companies across the United States to enhance security of surface transportation infrastructure through risk-based security assessments, critical infrastructure hardening, and close partnerships with state and local law enforcement partners.

Because of its open access architecture, surface transportation has a fundamentally different operational environment than aviation. As a result, our approach is necessarily different. To protect surface transportation, we have conducted compliance inspections throughout the freight rail and mass transit domains; critical facility security reviews for pipeline facilities; comprehensive mass transit assessments that focus on high-risk transit agencies; and corporate security reviews conducted in multiple modes of transportation on a continuous basis to elevate standards and identify security gaps.

We also have continued to support Visible Intermodal Prevention and Response (VIPR) teams, including 12 multi-modal teams. VIPR teams are composed of personnel with expertise in inspection, behavior detection, security screening, and law enforcement for random, unpredictable deployments throughout the transportation sector to prevent potential terrorist and criminal acts.

These efforts have been supported by more than $1.6 billion in DHS grant funding awarded through the Transit Security Grant Program to harden assets, improve situational awareness, and build national capabilities to prevent and respond to threats and incidents across the transportation sector.

Global Supply Chain Security

Securing the global supply chain system is integral to securing both the lives of people around the world, and maintaining the stability of the global economy. We must work to strengthen the security, efficiency, and resilience of this critical system. Supply chains must be able to operate effectively, in a secure and efficient fashion, in a time of crisis, recover quickly from disruptions, and continue to facilitate international trade and travel.

Earlier this year, I announced on the behalf of the President the U.S. National Strategy for Global Supply Chain Security. This new Strategy provides a government-wide vision of our goals, approach, and priorities to strengthen the global supply chain system. The Strategy establishes two explicit goals: promoting the efficient and secure movement of goods and fostering resilient supply chain systems. As we work to achieve these goals, we will be guided by the overarching principles of risk management and collaborative engagement with key stakeholders who also have key supply chain roles and responsibilities.

DHS is now working in close partnership with other federal departments and agencies to translate the high-level guidance contained in the Strategy into concrete actions. We are focusing our immediate efforts on the priority action areas identified in the Strategy. Some of these efforts include:

- Threat and Risk: Working in concert with other agencies to develop the nation's first Global Supply Chain Threat Assessment and Risk Characterization
- Information Sharing: advancing the development and government-wide utilization of the International Trade Data System for the collection, use, and dissemination of commercial data.
- Targeting Capabilities: Improving the capabilities of targeting systems used to identify high-risk cargo by obtaining additional information from stakeholders as early in the process as possible.
- Infrastructure Resilience: Exploring expanding DHS's Resilience STAR program into the transportation sector, to highlight and advance security and resiliency standards for key supply chain nodes and infrastructure.
- Partnership Programs: Reviewing the variety of US "public-private" partnership programs, with an eye towards

opportunities to harmonize them to enhance efficiencies, reduce costs, and better leverage federal resources.

- Technology: Prioritizing research and development needs, both within DHS and across the interagency, based upon an assessment of current capabilities and an understanding of evolving threats and vulnerabilities.

In addition to some of these specific efforts to implement the National Strategy for Global Supply Chain Security, DHS continues to advance a range of other measures and programs to strengthen different components of this vital system.

We are strengthening the global system by working with multilateral organizations such as the International Maritime Organization (IMO), the International Civil Aviation Organization (ICAO), the World Customs Organization (WCO), and the Asia-Pacific Economic Cooperation (APEC) as well as bilaterally with trading partners. Our efforts are not only directed toward achieving specific objectives within the organizations but also on promoting collaboration between them.

For example, we are working with the IMO, WCO, and APEC on developing global systems for managing trade recovery in the event of large scale disruptions. Our engagement with APEC has resulted in their identification of the specific information that governments and the private sector need to be ready to exchange in order to support trade recovery efforts.

We are also working closely with industry and foreign government partners to identify and address high-risk shipments as early in the shipping process as possible by collecting and analyzing advance electronic commercial data. This allows DHS to make risk informed decisions about what cargo is safe to be loaded onto vessels and aircraft prior to their departure from a foreign port and facilitates the clearance of those shipments upon their arrival in the United States.

In the aviation environment, we are working with leaders from global shipping companies and the International Air Transport Association (IATA) to develop preventive measures, including terrorism awareness training for employees and vetting personnel with access to cargo. We now allow participating shippers to screen air cargo, following strict standards to support the requirements of the 9/11 Act for cargo transported on passenger aircraft. We are reviewing our foreign partners' cargo screening to determine whether their programs provide a level of security commensurate with U.S. air cargo security standards. Those who meet these requirements are officially recognized to conduct screening for cargo traveling to the U.S., further strengthening the security of the global supply chain while facilitating the flow of legitimate commerce by screening cargo throughout the supply chain.

DHS is also focused on preventing the exploitation of the global supply chain by those seeking to use the system to transport dangerous, illicit, contraband, contaminated, and counterfeit products. Under Program Global Shield, just one example of these efforts, we are working with more than 80 countries to prevent the illegal theft or diversion of precursor chemicals that can be used to make Improvised Explosive Devices, or IEDs. Through these efforts we have already seized more than 62 metric tons of these deadly materials.

DHS, through ICE, also continues to investigate U.S. export control law violations, including those related to military items, controlled "dual-use" commodities, and sanctioned or embargoed countries. We are committed to making sure foreign adversaries do not illegally obtain U.S. military products and sensitive technology, including weapons of mass destruction and their components, or attempt to move these items through the global supply chain. In Fiscal Year 2011, ICE initiated 1,780 new investigations into illicit procurement activities, made 583 criminal arrests, and made 2,332 seizures valued at $18.9 million. ICE also manages and operates the Export Enforcement Coordination Center (E2C2), an interagency hub for streamlining and coordinating export enforcement activities and exchanging information and intelligence.

Countering Chemical, Biological, Radiological, and Nuclear Threats

Countering biological, nuclear, and radiological threats requires a coordinated, whole-of-government approach. DHS, through the Domestic Nuclear Detection Office (DNDO) and Office of Health Affairs (OHA), works in partnership with agencies across federal, state, and local governments to prevent and deter attacks using nuclear and radiological weapons through nuclear detection and forensics programs. OHA also provides medical and scientific expertise to support bio preparedness and response efforts.

Through the Securing the Cities program, for example, nearly 11,000 personnel in the New York City region have been trained in preventive radiological and nuclear detection operations and nearly 6,000 pieces of radiological detection equipment have been deployed. DNDO also has facilitated the delivery of radiological and nuclear detection training to more than 4,700 state and local officers and first responders.

Through the BioWatch program, an environmental surveillance system that provides early detection of biological agents, OHA has collected over 200,000 samples in more than 30 cities nationwide to enhance protection and preparedness for high-consequence biological threats. Last year, OHA also conducted the first-ever detailed testing on automated biodetection

systems for national application. These detectors analyze samples and relay results to public health officials, and will significantly reduce the time needed to detect a biological attack, potentially saving thousands of lives.

Last year, the DHS National Biodefense Analysis and Countermeasures Center (NBACC) laboratory, which is managed by DHS S&T, also received its accreditation with the Centers for Disease Control & Prevention (CDC) and the U.S. Department of Agriculture to begin research and diagnostics on pathogens to understand the scientific basis of the risks posed by biological threats and to attribute their use in bioterrorism events.

Under the leadership of the Office of Science and Technology Policy, DHS S&T, in collaboration with NIST, also published "The National Strategy for Chemical, Biological, Radiological, Nuclear, and Explosives (CBRNE) Standards," which lays out the federal vision and goals to achieve a comprehensive structure for the coordination, prioritization, establishment and implementation of CBRNE equipment standards by 2020.

Securing and Managing Our Borders

DHS secures the nation's air, land, and sea borders to prevent illegal activity while facilitating lawful travel and trade. The Department's border security and management efforts focus on three interrelated goals: effectively securing U.S. air, land, and sea borders; safeguarding and streamlining lawful trade and travel; and disrupting and, in coordination with other federal agencies, dismantling transnational criminal and terrorist organizations.

Southwest Border

To secure our nation's Southwest border, we have continued to deploy unprecedented amounts of manpower, resources, and technology, while expanding partnerships with federal, state, tribal, territorial, and local partners, as well as the Government of Mexico.

Simply put, the Obama administration has undertaken the most serious and sustained actions to secure the Southwest border in our nation's history. We have increased the number of Border Patrol agents nationwide from approximately 10,000 in 2004 to more than 21,000 today with nearly 18,500 "boots on the ground" along the Southwest border. Working in coordination with state and other federal agencies, we have deployed a quarter of all ICE operational personnel to the Southwest border region – the most ever – to dismantle criminal organizations along the border.

We have doubled the number of ICE personnel assigned to Border Enforcement Security Task Forces, which work to dismantle criminal organizations along the border. We have tripled deployments of Border Liaison Officers, who facilitate cooperation between U.S. and Mexican law enforcement authorities on investigations and enforcement operations, including drug trafficking (coordinated with the Drug Enforcement Administration). We also have increased the number of intelligence analysts working along the U.S.-Mexico border.

In addition, we have deployed dual detection canine teams as well as non-intrusive inspection systems, Mobile Surveillance Systems, Remote Video Surveillance Systems, thermal imaging systems, radiation portal monitors, and license plate readers to the Southwest border. These technologies, combined with increased manpower and infrastructure, give our personnel better awareness of the border environment so they can more quickly act to resolve potential threats or illegal activity. We also are screening southbound rail and vehicle traffic looking for the illegal weapons and cash that are helping fuel the cartel violence in Mexico.

We also have completed 650 miles of fencing out of nearly 652 miles mandated by Congress as identified by Border Patrol field commanders, including 299 miles of vehicle barriers and 351 miles of pedestrian fence.

To enhance cooperation among local, tribal, territorial, state and federal law enforcement agencies, we have provided nearly $205 million in Operation Stonegarden funding since 2009. In that time, Southwest border law enforcement agencies received over $167 million in grants through the Operation Stonegarden program.

Our work along the border has included effective support from our partners at the Department of Defense (DOD). In addition to continuing support from DOD's Joint Task Force-North and the National Guard, in 2010, President Obama authorized the temporary deployment of up to 1,200 National Guard troops to the Southwest Border to contribute additional capabilities and capacity to assist law enforcement agencies as a bridge to longer-term enhancements in the efforts to target illicit networks' smuggling of people, drugs, illegal weapons, money, and the violence associated with these illegal activities.

Beginning in March 2012, DOD's National Guard support to CBP began to transition from ground support to air support, essentially moving from boots on the ground to boots in the air with state of the art aerial assets equipped with the latest

detection and monitoring capabilities.

These aerial assets, which include both rotary and fixed-wing aircraft, supplement the CBP Office of Air and Marine aerial assets and support the Border Patrol's ability to operate in diverse environments, expand our field of vision in places with challenging terrain, and help us establish a greater visible presence from a distance, which increases deterrence.

The U.S. Coast Guard also is continuing its integral role in our border enforcement strategy through its maritime operations at the Joint Interagency Task Force (JIATF)-South, the U.S. Southern Command entity that coordinates integrated interagency counter drug operations, the Caribbean Sea, Gulf of Mexico, and the eastern Pacific. In Fiscal Year 2011, the Coast Guard removed nearly 75 metric tons of cocaine, and more than 17 metric tons of marijuana. CBP Office of Air and Marine P-3 aircraft also have been an integral part of successful counter-narcotic missions operating in the Source and Transit Zones in coordination with JIATF-South.

The results of these comprehensive and coordinated efforts have been striking. Border Patrol apprehensions—a key indicator of illegal immigration—have decreased 53 percent in the last three years and are less than 20 percent of what they were at their peak. Indeed, illegal immigration attempts have not been this low since 1971. Violent crime in U.S. border communities has also remained flat or fallen over the past decade, and statistics have shown that some of the safest communities in America are along the border. From Fiscal Years 2009 to 2011, DHS also seized 74 percent more currency, 41 percent more drugs, and 159 percent more weapons along the Southwest border as compared to Fiscal Years 2006 to 2008.

To further deter individuals from illegally crossing our Southwest border, we also directed ICE to prioritize the apprehension of recent border crossers and repeat immigration violators, and to support and supplement Border Patrol operations. Between Fiscal Years 2009 and 2011, ICE made over 30,936 criminal arrests along the Southwest border, including 19,563 arrests of drug smugglers and 4,151 arrests of human smugglers.

Over the past year we made several announcements that will continue to support this work and expand the collaboration necessary to sustain the progress we have achieved. For example, in July 2011, the Obama Administration released the 2011 National Southwest Border Counternarcotics Strategy, a key component of federal efforts to enhance security along the Southwest border. The strategy outlines federal, state, local, tribal, and international actions to reduce the flow of illicit drugs, cash, and weapons across the border, and highlights the Obama Administration's support for promoting strong border communities by expanding access to drug treatment and supporting programs that break the cycle of drug use, violence, and crime.

The *Declaration on 21st Century Border Management*, issued by President Obama and President Calderon last year, signals the United States government's commitment to increase collaboration with Mexico; both to facilitate legitimate trade and travel at the border and to continue combating transnational crime. As part of this effort, we are working closely with our Mexican counterparts on critical infrastructure protection and expansion of trusted traveler and shipper programs.

In addition to our efforts to strengthen border security, we made great strides in expediting legal trade and travel, working with local leaders to update infrastructure and reduce wait times at our Southwest border ports of entry. Along the Southwest border, new initiatives have included outbound infrastructure improvements and port hardening, which when completed, will expand our outbound inspection capabilities, enhance port security, and increase officer safety. We also have implemented Active Lane Management, which leverages Ready Lanes, Dedicated Commuter Lanes, and LED signage to dynamically monitor primary vehicle lanes and re-designate lanes as traffic conditions and infrastructure limitations warrant.

These efforts are not only expediting legitimate trade, they are also stopping contraband from entering and leaving the country. In Fiscal Year 2011, DHS interdicted goods representing more than $1.1 billion in Manufacturer's Suggested Retail Price. Further, the value of consumer safety seizures including pharmaceuticals totaled more than $60 million, representing a 41 percent increase over Fiscal Year 2010.

Northern Border

Along the Northern border, we have continued to deploy technology and resources to protect the border, invest in port of entry improvements to enhance security and improve trade and travel, and deepen our already strong partnership with Canada.

For instance, CBP expanded unmanned aerial surveillance coverage along the Northern border into eastern Washington, now covering 950 miles of the Northern border. In 2011, CBP Office of Air and Marine provided nearly 1,500 hours of unmanned aerial surveillance along the Northern Border.

In 2011, CBP also opened the Operations Integration Center in Detroit—a multi-agency communications center for CBP, DHS, and other federal, state, local, and Canadian law enforcement agencies on the northern border. The Operations Integration Center increases information sharing capabilities leading to seizures of drugs, money and illegal contraband along the U.S - Canada border within the Detroit Sector. S&T is also evaluating new surveillance technologies for CBP in Swanton Sector, Vermont that can operate in harsh and remote environments and use renewable energy such as solar and wind power. Sharing surveillance data with Canada to combat illegal border entries is also in progress.

We also have continued to invest heavily in infrastructure improvements at our ports of entry, including over $400 million in Recovery Act funds to modernize older facilities along our Northern border to meet post-9/11 security standards.

Through the Beyond the Border Action Plan released by President Obama and Prime Minister Harper in December 2011, we are also enhancing cooperation with Canada through greater information sharing, more coordinated passenger and baggage screening, and integrated law enforcement operations. .As part of this action plan, we are working with our U.S. and Canadian partners to develop the next generation of integrated cross-border law enforcement, interoperable radio communications, border wait time measurements, and enhanced air/land/maritime domain awareness, as well as a multitude of initiatives to streamline trusted trader and traveler programs and expedite legitimate travel and trade.

With Canada's Public Safety Minister Vic Toews, I announced the Joint Border Threat and Risk Assessment, highlighting our nations' shared commitment to identifying and mitigating potential threats of terrorism and transnational organized crime along the border.

Enforcing and Administering our Immigration Laws

DHS has undertaken a historic effort to enforce and administer immigration laws in a cohesive way that is smart, effective, and that maximizes the resources that the Congress has given us to do this important job. We have worked, and continue to work, to make sure that our limited resources are applied consistently and in a manner that enhances public safety, border security, and the integrity of the immigration system, while respecting the rule of law and staying true to our history as a nation of immigrants.

Targeting Criminal and Other Priority Aliens

We have established as a top priority the identification and removal of public safety and national security threats. To this end, we have expanded the use and frequency of investigations and programs that track down criminals and other public safety and national security threats on our streets and in our jails.

Overall, in Fiscal Year 2011, ICE removed nearly 397,000 individuals. Ninety percent of these removals fell within one of ICE's priority categories, and 55 percent, or more than 216,000 of the people removed, were convicted criminal aliens – an 89 percent increase in the removal of criminals from Fiscal Year 2008. This total includes more than 87,000 individuals convicted of homicide, sexual offenses, dangerous drugs, and driving under the influence. Of those removed in Fiscal Year 2011 without a criminal conviction, more than two-thirds fell into our priority categories of recent border crossers or repeat immigration law violators.

In a single "Cross Check" enforcement operation conducted over a six-day period this year, ICE arrested more than 3,100 convicted criminal aliens, immigration fugitives and immigration violators. This operation was the largest of its kind, involving the collaboration of more than 1,900 ICE officers and agents. Arrests occurred in all 50 states, four U.S. territories, and the District of Columbia.

Through the Secure Communities program, ICE uses biometric information to identify criminal and other priority aliens found in state prisons and local jails so that ICE can prioritize them for removal. It remains an important tool in ICE's efforts to focus its immigration enforcement resources on individuals within ICE's priorities, particularly those who pose a threat to public safety or national security.

We have expanded the Secure Communities program from 14 jurisdictions in 2008 to 2,304 today, including all jurisdictions along the Southwest border. We are on track to deploy this program to all jurisdictions nationwide by 2013. Since its inception, more than 135,400 immigrants convicted of serious crimes, including aggravated felony offenses like murder, rape and sexual abuse of children, have been removed from the United States after identification through Secure Communities.

Nevertheless, we recognize that there is always room to improve any program, and we are mindful of concerns raised about Secure Communities. Under the leadership of ICE Director John Morton, we have taken significant action to improve the program and clarify its goals to law enforcement and the public.

We are committed to ensuring the Secure Communities program respects civil rights and civil liberties. To that end, ICE is working closely with law enforcement agencies and stakeholders across the country to ensure the program operates in the most effective manner possible and respects community policing efforts critical to public safety. ICE and CRCL are developing videos for state and local law enforcement agencies on how Secure Communities works and how it relates to laws governing civil rights and civil liberties. They also are conducting a regular statistical analysis of the program to identify any signs of potential abuse, and they have announced a complaint investigation protocol where individuals or organizations who believe civil rights violations connected to Secure Communities have occurred can file a complaint with ICE or CRCL. We also are reviewing the findings and recommendations of the DHS Homeland Security Advisory Council (HSAC) Secure Communities Task Force.

In addition, as part of its enforcement approach, ICE has issued additional guidance to its personnel to ensure that those enforcing immigration laws make appropriate use of the discretion they already have in deciding the types of individuals we prioritize for removal from the country. President Obama and I have both made clear that we will continue to enforce the laws in a smart and effective manner, and part of this is exercising discretion on a case by case basis where DHS feels it enhances our ability to meet our priorities.

With the cooperation of the Department of Justice, we continue to review incoming cases and existing caseloads to ensure they correspond with our enforcement priorities and support our mission to protect public safety and ensure border security. This effort has led to an unprecedented collaboration among federal agencies to focus taxpayer resources devoted to immigration enforcement on priority cases.

Deterring Employment of Aliens Not Authorized to Work

In the worksite category, we have eliminated high-profile raids that did little to enhance public safety, instead promoting compliance with worksite-related laws through criminal prosecutions of egregious employer violators, Form I-9 inspections, civil fines, and debarment, as well as education and compliance tools.

Since January 2009, ICE has audited more than 7,001 employers suspected of knowingly hiring workers unauthorized to work in the United States, debarred 594 companies and individuals, and imposed more than $79.9 million in financial sanctions—more than the total amount of audits and debarments during the entire previous administration.

Employer enrollment in E-Verify, our on-line employee verification system managed by U.S. Citizenship and Immigration Services (USCIS), has more than doubled since January 2009, with more than 358,000participating companies representing more than 1.1 million hiring sites. USCIS has continued to promote and strengthen E-Verify, developing a robust customer service and outreach staff to increase public awareness of E-Verify's benefits and inform employers and employees of their rights and responsibilities. In Fiscal Year 2011 alone, USCIS informed tens of millions of people about E-Verify through radio, print, and online ads in English and Spanish, and hundreds of thousands more through live presentations, conference exhibitions, live webinars, and distribution of informational materials.

More than 17 million queries were processed in E-Verify in Fiscal Year 2011, allowing businesses to verify the eligibility of their employees to work in the United States. Last year, we also launched the E-Verify Self Check program, a voluntary, free, fast, and secure online service that allows individuals in the United States to confirm the accuracy of government records related to their employment eligibility status before seeking employment.

Detention Reform

As a part of ongoing detention reform efforts, ICE continues to identify systematic ways to reform and improve medical and mental health care at detention facilities, including an increase in medical case management and quality management activities, assigning field medical coordinators to each ICE Field Office to provide ongoing case management; simplifying the process for detainees to receive authorized health care treatments; and developing a medical classification system to support detainees with unique medical or mental health needs.

ICE also has issued revised detention standards. The new standards, known as Performance-Based National Detention Standards 2011 (PBNDS 2011), reflects ICE's ongoing effort to tailor the conditions of immigration detention while maintaining a safe and secure detention environment for staff and detainees. In developing the revised standards, ICE incorporated the input of many agency employees and stakeholders, including the perspectives of nongovernmental organizations and ICE field offices. PBNDS 2011 is crafted to improve medical and mental health services, increase access to legal services and religious opportunities, improve communication with detainees with limited English proficiency, improve the process for reporting and responding to complaints, detect and prevent sexual assault and abuse, and increase visitation.

ICE has hired additional detention service managers to increase onsite federal oversight and ensure that facilities are in compliance with its detention standards while increasing announced and unannounced inspections by other staff. CRCL has assisted in training these ICE employees and reviewing the standards they enforce. CRCL has also stepped up oversight of immigration facilities, conducting numerous on-site inspections, and additional reviews specifically relating to medical care.

Additionally, instead of housing the vast majority of immigrant detainees in small groups in jails across the country, ICE has initiated a consolidation effort which includes the addition of larger, civil detention facilities to its inventory.

Last year, ICE opened two such facilities in California and New Jersey and opened the first true civil detention facility in Texas in February 2012. The acquisition of these facilities has enabled ICE to reduce the number of transfers and detain individuals closer to their arrest locations, families, legal service providers, and other community support organizations.

ICE will continue building on these ongoing detention reform efforts. It expects to implement a new Risk Classification Assessment nationwide to improve transparency and uniformity in detention custody and classification decisions and to promote identification of vulnerable populations. In addition, ICE will continue its implementation of the new Transfer Directive, which is designed to minimize long-distance transfers of detainees within ICE's detention system, especially for those detainees with family members, local attorneys, or pending immigration proceedings in the area where they are detained.

Improving Legal Immigration

Our nation's founding is rooted in immigration and immigrants have contributed to the richness of our culture, the strength of our character, and the advancement of our society. To continue to promote legal immigration to the United States and the process by which we naturalize new American citizens each year, we have worked to reduce bureaucratic inefficiencies in visa programs, streamline the path for entrepreneurs who wish to bring their business to America, and improve our systems for providing immigration benefits and services.

In 2011, USCIS held more than 6,000 naturalization ceremonies for approximately 692,000 lawful permanent residents who became U.S. citizens, including more than 10,000 members of the U.S. Armed Forces.

To help combat fraud and exploitation of our immigration system, USCIS launched the Unauthorized Practice of Immigration Law (UPIL) initiative, a national, multi-agency campaign that spotlights immigration-services scams and the problems that can arise for immigrants when legal advice or representation is given by people who are not attorneys or accredited representatives. The UPIL initiative began in seven cities in 2011 and will expand nationwide in 2012.

USCIS also launched a series of policy, operational, and outreach efforts to support economic growth and stimulate investment by attracting foreign entrepreneurs who can create jobs, form startup companies, and invest capital in areas of high unemployment.

USCIS also announced the Entrepreneurs in Residence initiative to ensure that its policies and practices better reflect business realities of industries that regularly use visa categories for immigrant investors, job-creating entrepreneurs, and workers with specialized skills, knowledge, or abilities.

These efforts have included enhancements to streamline the Employment Creation immigrant visa program, commonly known as the EB-5 Program, including conducting a top to bottom review of EB-5 business processes, and hiring economists and business analysts to support EB-5 adjudications.

USCIS also has provided clarification on how H-1B visas, which allow U.S. employers to temporarily employ foreign workers in specialty occupations, and EB-2 National Interest Waivers, which offer a streamlined eligibility for immigrant visas to certain foreign workers with advanced degrees and/or exceptional ability in the arts, sciences, or business, may be utilized by foreign-born entrepreneurs.

In addition, last year USCIS launched the Citizenship Public Education and Awareness Initiative to promote awareness of the rights, responsibilities and importance of U.S. citizenship and the free naturalization preparation resources available to permanent residents and immigrant-serving organizations. This multilingual effort is designed to reach nearly 8 million permanent residents eligible to apply for citizenship. And in September 2011, USCIS awarded $9 million in Citizenship and Integration Grants to 42 organizations to expand citizenship preparation programs for permanent residents across the country. The President's Fiscal Year 2013 budget request includes $11 million to continue support for USCIS immigrant integration efforts through funding of citizenship and integration program activities including competitive grants to local immigrant-serving organizations to strengthen citizenship preparation programs for permanent residents.

In January, USCIS also proposed a regulatory change that would significantly reduce the time that U.S. citizens are separated from their spouses and children as they go through the process of obtaining visas to become legal immigrants to the United States. The proposed rule change would minimize the extent to which delays separate Americans from their families by allowing family members, under certain circumstances, to have their waiver applications processed in the United States and receive a provisional waiver determination before they complete the visa process outside the United States.

USCIS also has made significant strides in the development of its Electronic Immigration System (ELIS) to begin the agency's transition from a paper-based to an electronic, online organization. USCIS is currently testing the system and will begin its public releases this year.

And to further enhance our nation's economic, scientific and technological competitiveness, last year I also announced the launch of the Study in the States initiative, an effort aimed at encouraging the best and the brightest international students from around the world to study in the U.S. by finding new and innovative ways to streamline the international student visa process. As part of the initiative, the Study in the States website provides coordinated information in a comprehensive, user-friendly, and interactive way to prospective and current international students, exchange visitors and their dependents about opportunities to study in the United States and learn about expanded post-graduate opportunities.

In March 2012, I also announced the formation of the Homeland Security Academic Advisory Council (HSAAC), comprised of university presidents and academic leaders who will provide advice and recommendations to me and senior DHS leadership on issues related to student and recent graduate recruitment, international students, academic research, campus and community resiliency, security and preparedness, and faculty exchanges.

Safeguarding and Securing Cyberspace

Our daily life, economic vitality, and national security depend on a safe, secure, and resilient cyberspace. A vast array of interdependent IT networks, systems, services, and resources are critical to communication, travel, powering our homes, running our economy, and obtaining government services.

DHS is the federal government's lead agency for securing civilian government computer systems and works with our industry and state, local, tribal, and territorial government partners to secure critical infrastructure and information systems. DHS analyzes and mitigates cyber threats and vulnerabilities; distributes threat warnings; provides solutions to critical research and development needs; and coordinates the vulnerability, mitigation, and consequence management response to cyber incidents to ensure that our computers, networks, and information systems remain safe.

The United States confronts a dangerous combination of known and unknown vulnerabilities in the cyber domain, strong and rapidly expanding adversary capabilities, and limited threat and vulnerability awareness. While we are more network dependent than ever before, increased interconnectivity increases the risk of theft, fraud, and abuse. No country, industry, community or individual is immune to cyber risks.

Cyber incidents have increased dramatically over the last decade. There have been instances of theft and compromise of sensitive information from both government and private sector networks, undermining confidence in our systems, information sharing processes, and the integrity of the data contained within these systems. Last year, the DHS U.S. Computer Emergency Readiness Team (US-CERT) received more than 100,000 incident reports, and released more than 5,000 actionable cybersecurity alerts and information products.

Recognizing the serious nature of this challenge, President Obama made cybersecurity an Administration priority upon taking office. In his Cyberspace Policy Review in 2009, which established a strategic framework for advancing the Nation's cybersecurity policies, the President declared that the "cyber threat is one of the most serious economic and national security challenges we face as a nation."

DHS works with federal agencies to secure unclassified federal civilian government networks and works with owners and operators of critical infrastructure to secure their networks through risk assessment, mitigation, and incident response capabilities.

To protect Federal civilian agency networks, we are deploying technology to detect and block intrusions in those agencies with support from interagency partners. We also work to provide agencies with assistance in the implementation of guidance and standards issued by NIST. In addition, DHS is responsible for coordinating the national response to significant cyber incidents, consistent with the National Response Framework, and for creating and maintaining a common operational picture for cyberspace across the government.

With respect to critical infrastructure, DHS and the sector specific agencies work with the private sector to help secure the key systems upon which Americans rely, such as the financial sector, the power grid, water systems, and transportation networks. We do this by sharing actionable cyber threat information with the private sector, helping companies to identify vulnerabilities before a cyber incident occurs, and providing forensic and remediation assistance to help response and recovery after we learn of a cyber incident.

Last year, the DHS Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) conducted 78 assessments of control system entities which helped companies identify security gaps and prioritize mitigations. We also empower owners and operators to help themselves by providing a cyber self-evaluation tool, which was utilized by over 1,000 companies last year, as well as in-person and on-line training sessions.

In addition, DHS S&T works collaboratively across federal agencies, private industry, academic networks and institutions, and global information technology owners and operators to research, develop, test, and transition deployable solutions to secure the nation's current and future cyber and critical infrastructures. For example, S&T is partnering with the Financial Services Sector Coordinating Council (FSSCC) to provide identity proofing solutions at financial institutions in order to reduce identity impersonation. The Financial Institution- Verification of Identity Credential Service (FI-VICS) effort is focused on creating a single interface from financial institutions to authoritative identity credential issuers (such as state Department of Motor Vehicles) to provide required authentication and authorizations between the financial institution requester and government identity credential issuer.

To combat cyber crime, DHS works with the Federal Bureau of Investigation and leverages the skills and resources of the U.S. Secret Service, ICE, and CBP to support prosecutions of cyber criminals brought by the Department of Justice. In Fiscal Year 2011 alone, DHS prevented $1.5 billion in potential losses through cyber crime investigations, resulting in prosecutors bringing charges against 72 individuals for their alleged participation in an international criminal network that sought the sexual abuse of children and the creation and dissemination of graphic images and videos of child sexual abuse throughout the world.

DHS also serves as a focal point for national cybersecurity outreach, cyber awareness, and workforce development efforts. Raising the cyber education and awareness of the general public creates a more secure environment in which the personal or financial information of individuals is better protected. DHS recognizes that partnership and collaboration are crucial to ensuring that all Americans take responsibility for their actions online. To that end, we are continuing to grow the Department's ***Stop.Think.Connect.™*** Campaign, which is a year-round national public awareness effort designed to engage and challenge Americans to join the effort to practice and promote safe online practices.

As we perform this work, we are mindful that one of our missions is to ensure that privacy, confidentiality, and civil liberties are not diminished by our efforts. The Department has implemented strong privacy and civil rights and civil liberties standards into all its cybersecurity programs and initiatives from the outset to ensure the highest standards of transparency and accountability. DHS has performed Privacy Impact Assessments (PIAs) of our key cybersecurity programs such as EINSTEIN, which provides intrusion detection capabilities to the civilian federal agencies. DHS also receives regular counsel on cybersecurity activities from the Data Privacy and Integrity Advisory Committee (DPIAC), a body of outside experts who advise the Department on ways to address privacy and civil liberties concerns. This year, US-CERT and CRCL also launched a training effort for all US-CERT personnel focused on identifying and preventing civil rights and civil liberties issues in US-CERT's cybersecurity activities.

The Department of Defense is a key partner in our cybersecurity mission. In 2010, I signed a Memorandum of Understanding with then-Secretary of Defense Robert Gates to formalize the interaction between DHS and DOD to protect against threats to our critical civilian and military computer systems and networks. Congress mirrored this division of responsibilities in the National Defense Authorization Act for Fiscal Year 2012. We are currently working with the Defense Industrial Base as well as other critical infrastructure sectors, such as the Banking and Finance Sector, to exchange actionable information about malicious activity.

While the Administration has taken significant steps to protect against evolving cyber threats, we must acknowledge that the current threat outpaces our current authorities. DHS executes its portion of the cybersecurity mission under an amalgam of existing statutory and executive authorities that fail to keep up with the responsibilities with which we are charged. Our cybersecurity efforts have made clear that our nation cannot improve its ability to defend against cyber threats unless certain laws that govern cybersecurity activities are updated.

In May 2011, the Obama Administration provided a pragmatic and focused cybersecurity legislative proposal for Congress to consider. We believe this proposal, as well as the Cybersecurity Act of 2012, provide important steps in improving the

cybersecurity posture of the United States. I hope that the current legislative debate maintains the bipartisan tenor it has benefitted from so far, and builds from the consensus that spans two Administrations and Congress' efforts of the last several years.

All sides agree that federal and private networks must be better protected, and information about cybersecurity threats should be shared more easily while ensuring that privacy and civil liberties are protected through a customized framework of information handling policies and oversight. Both the Administration's proposal and the bi-partisan Cybersecurity Act of 2012 currently before the Senate would improve operations in those areas by providing DHS with clear statutory authority commensurate with our cybersecurity responsibilities, although the Administration would still like to discuss certain concerns with specific parts of the Cybersecurity Act of 2012.

In addition, many agree with the House Republican Cyber Task Force when it said, "Congress should consider carefully targeted directives for limited regulation of particular critical infrastructures to advance the protection of cybersecurity." Both the Administration's proposal and the Senate legislation recognize the severity and urgency to secure critical infrastructure and take some basic steps in this area.

Accordingly, the Administration has proposed risk mitigation guidance to ensure that companies providing the Nation's most essential services are instituting a baseline level of cybersecurity. This proposal would leverage the expertise of the private sector requiring the Nation's most critical infrastructure adopt the cybersecurity practices, technologies, and performance standards that work best on their networks.

There is also broad support for increasing the penalties for cyber crimes and for creating a uniform data breach reporting regime to protect consumers. The Administration's proposal will help protect the American people by enhancing our ability to prosecute cyber criminals and by establishing national standards requiring businesses that have suffered an intrusion to notify affected individuals if the intruder had access to the consumers' personal information.

I believe we have made great progress toward reaching a consensus that will help protect the American people, Federal government networks and systems, and our Nation's critical infrastructure. The time to act is now: to improve cybersecurity coordination, strengthen our cybersecurity posture, and protect all elements of our economy against this serious and growing threat, while protecting privacy, confidentiality, and civil liberties.

Conclusion

We have come a long way over the past year, and in the ten years since 9/11, to enhance protection of the United States and engage our full range of partners in this shared responsibility. Together, we have made significant progress to better secure our country, but we are aware of the challenges that remain.

Threats against our nation, whether by terrorism or otherwise, continue to exist and evolve. And DHS must continue to evolve as well. We continue to be ever vigilant to protect against terrorist attacks while promoting the movement of goods and people and protecting our essential rights and liberties.

I thank the Committee for your continued partnership and guidance as together we work to keep our nation safe. I look forward to your questions.

This page was last reviewed/modified on April 25, 2012.