Statement for the Record

"Homeland Threats and Agency Responses"

Secretary Janet Napolitano

U.S. Department of Homeland Security

Before the

United States Senate

Committee on Homeland Security and Governmental Affairs

September 19, 2012

Thank you, Chairman Lieberman, Ranking Member Collins, 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), not only over the past three and a half years, but indeed, since the Department's founding. I look forward to continuing our work together to protect the American people as we advance our many shared goals.

I also thank Director Mueller and Director Olsen. DHS collaborates very closely and effectively with the Federal Bureau of Investigation (FBI) and National Counterterrorism Center (NCTC), and together we have forged a strong partnership to meet the shared responsibility of protecting the American people from foreign terrorist plots to acts of homegrown extremists.

Eleven years after the terrorist attacks of September 11th, 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. I thank them all for their service.

Created with the founding principle of protecting the American people from terrorist and other threats, DHS and its many partners across the Federal government, public and private sectors, and communities throughout the country have strengthened homeland security to better mitigate and defend against evolving threats.

Additionally, within the Federal government, many departments and agencies contribute to the homeland security mission. The Nation's armed forces serve on the frontlines of homeland security by degrading al-Qaeda's capabilities to attack the United States and targets throughout the world. The Office of the Director of National Intelligence, the Central Intelligence Agency, and the entire Intelligence Community, of which DHS is a member, are producing better streams of intelligence than at any time in history.

The Federal homeland security enterprise also includes the strong presence of the Department of Justice (DOJ) and the FBI, whose role in leading terrorism investigations has led to the arrest of numerous individuals on terrorism-related charges.

But despite considerable progress, the recent attacks in Oak Creek, Wisconsin, and Aurora, Colorado—and the terrorist attack in Bulgaria—serve as a reminder that our work to detect and prevent attacks is never done.

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 citizens, 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. We have also supported and sustained preparedness and response capabilities across the country through more than $36 billion in homeland security grants since 2002.

As we look ahead, and in order to address evolving threats and make the most of limited resources, the Administration proposed a new vision for homeland security grants in the Fiscal Year (FY) 2013 President's budget. The Administration's proposal focuses on building and sustaining core capabilities associated with the five mission areas within the National Preparedness Goal (NPG), helping to elevate nationwide preparedness.

This proposal reflects the many lessons we have learned in grants management and execution over the past ten years. Using a competitive, risk-based model, the proposal envisions a comprehensive process to assess gaps, identify and prioritize 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. The Administration looks forward to working with Congress and stakeholders on this proposal to enable all levels of government to build and sustain, in a collaborative way, the core capabilities necessary to prepare for incidents that pose the greatest risk to the security of the Nation.

Our experience over the past several years has also made us smarter about the terrorist threats we face and how best to deal with them. We 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 provide security that is seamless and efficient.

We also free up more time and resources, giving us the ability to focus resources on those threats or individuals we know the least about. This approach not only makes us safer, it also creates efficiencies within the system for travelers and for businesses. In other words, our homeland security and our economic security go hand-in-hand.

Strengthening homeland security includes a significant international dimension. To most effectively carry out our core missions – including preventing terrorism, securing our borders, 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 the State Department and 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, to help 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, and our vision for working with 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 terrorists—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, foiled attacks against air cargo, and other attempts across the country. Nonetheless, recent attacks overseas, and the continued threat of homegrown terrorism in the United States, demonstrate how we must 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.

Likewise, countering biological, chemical, nuclear, and radiological threats requires a coordinated, whole-of-government approach. DHS, through the Domestic Nuclear Detection Office, 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. The Office of Health Affairs (OHA), the Science and Technology Directorate (S&T), and the Federal Emergency Management Agency (FEMA) also provide medical, scientific, and other technical expertise to support chemical, biological, nuclear, and radiological preparedness and response efforts.

Sharing Information, Expanding Training, and Raising Public Awareness

The effective sharing of information in a way that is timely, actionable whenever possible, and that 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 outdated color-coded alert system with the 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 the Nation's 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. DHS also has provided hundreds of personnel, including U.S. Immigration and Customs Enforcement (ICE) special agents, U.S. Secret Service (USSS) agents, Federal Air Marshals, U.S. Customs and Border Protection (CBP) officers, U.S. Citizenship and Immigration Services (USCIS) officers, and representatives from FEMA and the U.S. Coast Guard (USCG) to support FBI-led Joint Terrorism Task Forces (JTTFs) across the country.

We are 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, increase opportunities for training and professional development for state and local analysts, and encourage the development of joint products between fusion centers and Federal partners.

Over the past three years, we have transformed how we train our Nation's frontline officers regarding suspicious activities, through the Nationwide Suspicious Activity Reporting Initiative (NSI). This initiative, which we conduct in partnership with the DOJ, is an Administration effort to train state and local law enforcement to recognize behaviors and indicators potentially related to terrorism and terrorism-related crime; standardize how those observations are documented and analyzed; and ensure the sharing of those reports with fusion centers for further analysis and with the JTTFs for further analysis and investigation.

As of August 2012, more than 234,000 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, we have also 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, transportation systems, universities, professional and amateur sports leagues and teams, entertainment venues, some of our Nation's largest retailers, as well as local law enforcement. Most recently DHS has partnered with sports leagues such as the National Football League, Major League Soccer, Major League Baseball, the National Basketball Association, National Collegiate Athletic Association, National Hockey League,

U.S. Golf, and the U.S. Tennis Association, to promote public awareness of potential indicators of terrorism at sporting events.

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 through extensive analysis and research on the behaviors and indicators of violent extremism. We are bolstering efforts to address the dynamics of violent extremism by strengthening partnerships with state, local, and international partners. And, we are expanding support for information-driven, community-oriented policing efforts through training and grants.

All of this work is consistent with the Administration's CVE Strategy released in August 2011 and the CVE *Strategic Implementation Plan (SIP) for Empowering Local Partners to Prevent Violent Extremism in the United States* released in December 2011.

As part of our CVE approach, DHS has conducted extensive analysis and research to better understand the threat of violent extremism in order to support state and local law enforcement, fusion centers, and community partners with the knowledge needed to identify behaviors and indicators associated with acts of violent extremism.

In addition, over the past year, DHS has worked closely with state and local partners, including the State and Provincial Police Academy Directors (SPPADS), the International Association of Chiefs of Police (IACP), the Major City Chiefs Association (MCC), the Major City Sheriff's Association (MCSA), as well as NCTC, DOJ, and the FBI to develop training for frontline law enforcement officers on behaviors potentially indicative of violent extremist activity.

DHS has also created a new CVE Webportal, launched on August 31, 2012, for a select group of law enforcement through the Homeland Security Information Network (HSIN). The purpose of this portal is to provide law enforcement with CVE training resources and materials, as well as a central portal for communication and information sharing on CVE. DHS aims to make the Webportal available to law enforcement nationwide by the end of September 2012.

Finally, DHS has supported State and Local CVE activities through grants. DHS publicly released the *CVE Training Guidance and Best Practices,* which was sent to all state and local partner grantors and grantees thereby tying CVE to grant guidance policy on October 7, 2011. DHS also incorporated language into FY 2012 grant guidance that prioritizes CVE and allows funds to be used in support of state and local CVE efforts.

Active Shooter Threats

There have been a series of international and domestic violent extremist incidents over the past several years that have involved active shooters, including the 2008 Mumbai attacks; shootings in 2009 at the U.S. Holocaust Memorial Museum, Fort Hood, and a military recruiting station in Little Rock, Arkansas; and the 2011 attacks in Utoya, Norway. The recent shooting at a Sikh temple in Oak Creek, Wisconsin, was carried out by an individual with a history of involvement in the white supremacist extremist movement, although his motives remain unknown. Attacks by active shooters with no known ties to extremist movements also have caused significant loss of life and injury, including most recently in Aurora, Colorado.

Preventing and responding to active shooter threats is a priority for state and local law enforcement authorities, regardless of the motivation behind the attack. Where there is any active shooter scenario, prevention is a priority, response efforts will be the same, and the impact on the community is significant. This is an area in which DHS, in partnership with the FBI, has been very active. DHS is working to better understand the behaviors and indicators that lead to these acts of violence, the tactics used, and the actions that can be taken to help prevent them in the future. A central goal of our efforts is to build capabilities within state and local law enforcement communities to effectively respond to active shooter threats.

As part of this effort, we have worked with the FBI to produce both classified and unclassified case studies about past active shooter events and have made them available to state and local law enforcement. These case studies include behaviors and indicators, so that front line personnel will be better able to recognize pre-incident indicators of an emerging active shooter threat. We have incorporated this information in the training materials pertaining to CVE.

Additionally, the DHS Office of Infrastructure Protection and FEMA conduct active shooter trainings for state and local law enforcement and for the private sector. DHS's Active Shooter Awareness Program provides resources to help public and private-sector security managers train their workforce and enhance their facilities' preparedness and response to an active shooter scenario. Since the program's inception in December 2008, more than 5,000 law enforcement officers and other partners have participated.

FEMA, through Louisiana State University, a member of the National Domestic Preparedness consortium, also offers the Law Enforcement Active Shooter Emergency Response (LASER) course which addresses the technical aspects of planning and implementing a rapid law enforcement deployment to an active shooter incident.

In addition, the Federal Law Enforcement Training Center (FLETC) has been instrumental in preparing our Nation's state, local, and Federal law enforcement officers to respond effectively to an active shooter incident should one occur. FLETC has trained over 4,000 U.S. law enforcement officers in active shooter response and active shooter response instructor training. These newly trained instructors have gone on to train thousands more. FLETC also has reached out to its law enforcement partners that have experienced active shooter incidents to develop "lessons learned/lesson anticipated" that help to continually update and improve the tactics for active shooter response programs.

DHS also has developed an online Independent Study Course titled "Active Shooter: What You Can Do" through FEMA's Emergency Management Institute. This course provides guidance to individuals, including managers and employees, to prepare to respond to an active shooter situation. Nearly 134,000 government and private-sector participants have completed this training since it was released in March 2011.

In collaboration with the FBI and NCTC, DHS and FEMA have organized a two-day Joint Counterterrorism Awareness Workshop Series (JCTAWS) to review and improve operational capabilities, response resources, and information sharing among Federal, state, local, and private sector partners. This nationwide initiative is designed to increase the ability of local jurisdictions to prepare for, protect against, and respond to coordinated terrorist attacks against multiple targets. Since 2011, workshops have been conducted in Boston, Philadelphia, Honolulu, Indianapolis, Sacramento, Houston, Nashville, Denver, and Los Angeles. Modified workshops were also conducted in Tampa and Charlotte in support of the Republican and Democratic National Conventions. The next scheduled workshop is in Las Vegas this October.

Because faith-based communities have been the targets of violence, DHS continues to maintain regular contact with faith-based communities and helps coordinate rapid incident communications efforts. One recent example includes the DHS Office for Civil Rights and Civil Liberties' (CRCL) activation of the Incident Community Coordination Team (ICCT) on August 6, 2012, following the shooting in Oak Creek, Wisconsin.

During the call, leaders from Sikh, Hindu, Jewish, Muslim, and interfaith communities and organizations discussed the shooting with senior Government officials from the White House, DOJ, FBI, and DHS. More than 100 participants from across the country joined the ICCT call to share information about response activities and resources available, and to address community concerns.

Through the Office of Infrastructure Protection, DHS also has made the Active Shooter Awareness Program available to faith-based communities, as well as provided resources to ensure that their facilities are safe and secure through site assessments, threat briefings, and trainings.

Protecting Our Aviation System

Threats to our aviation system remain active and continue to evolve. Consequently, the Transportation Security Administration (TSA) is working internationally and with the private sector to continue to improve security screening, while simultaneously facilitating lawful travel and trade. We are continuing 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 shift aviation security from a "one size fits all" approach for passenger screening to a risk-based approach. In doing so, TSA utilizes a range of measures, both seen and unseen, as part of its layered security system - from state of the art

explosives detection, to using Advanced Imaging Technology (AIT) units and canine teams to screen passengers and cargo, to expediting screening for known travelers. 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.

In our increasingly interconnected world, we also work beyond our own airports, partnering with our Federal agencies and countries to protect both national and economic security.

For example, through the Pre-Departure Targeting Program, Immigration Advisory Program and enhanced in-bound targeting operations, Customs and Border Protection (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, 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 Officers deployed overseas inspect passengers abroad 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.

Finally, our continued use, analysis, and sharing of Passenger Name Record (PNR) data has allowed us to better identify passengers who merit our attention before they depart for the U.S. On July 1, 2012, a new agreement with the European Union on the transfer of PNR data entered into force, marking an important milestone in our collective efforts to protect the international aviation system from terrorism and other threats.

As we have taken these actions to strengthen security, we also have focused on expediting lawful 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 CBP, is allowing us to expedite entry into the United States for pre-approved, low-risk air travelers. More than one million trusted traveler program members are able to use the Global Entry kiosks, and we are expanding the program both domestically and internationally as part of the Administration's efforts to foster increased travel and tourism.

In addition to U.S. citizens and lawful permanent residents, Mexican nationals can now enroll in Global Entry, and Global Entry's benefits are also available to Dutch citizens enrolled in the Privium program; South Korean citizens enrolled in the Smart Entry Service program; Canadian citizens and residents through the NEXUS program; and citizens of the United Kingdom, Germany, and Qatar through limited pilot programs. In addition, we have signed agreements with Australia, New Zealand, Panama, and Israel to allow their qualifying citizens to participate in Global Entry. We are continuing to expand the program both domestically and internationally as part of the Administration's efforts to foster travel and tourism, which supports the President's Executive Order 13597 on Travel and Tourism.

U.S. citizen participants in Global Entry are also eligible for TSA Pre✓™ – a passenger prescreening initiative. TSA Pre✓™ is part of the agency's ongoing effort to implement risk-based security concepts that enhance security by focusing on travelers the agency knows least about. More than 2 million passengers have received expedited screening through TSA Pre✓™ security lanes since the initiative began last fall. TSA Pre✓™ is now available in 25 airports for select U.S. citizens traveling on Alaska Airlines, American Airlines, Delta Air Lines, United Airlines and US Airways and members of CBP Trusted Traveler programs. TSA has expanded TSA Pre✓™ benefits to U.S. military active duty members traveling through Ronald Reagan Washington National and Seattle-Tacoma international airports. In addition to TSA Pre✓™, TSA has implemented other risk-based security measures including modified screening procedures for passengers 12 and younger and 75 and older.

Visa Waiver Program

With our partners overseas, we have acted to strengthen the Visa Waiver Program (VWP), a program that boosts our economy by facilitating legitimate travel for individuals traveling to the United States for tourism or business. According to the Commerce Department, tourism alone supported 7.6 million U.S. jobs last year, and tourism revenue in early 2012 was up 14 percent from the previous year.

The VWP is an essential driver of international tourism because it 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. Almost two-thirds of international travelers come to the U.S. from VWP countries. Additionally, since its inception in the mid-1980s, VWP has also 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, in collaboration with the DOJ, has concluded Preventing and Combating Serious Crime (PCSC) agreements, or their equivalent, with 35 VWP countries and two VWP aspirants. DHS, along with the Departments of Justice and State, continues to work closely with the remaining country to sign a PCSC agreement. These agreements facilitate the sharing of information about terrorists and serious criminals. The U.S. government has also concluded negotiations on arrangements with all VWP countries for the exchange of terrorism screening information.

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.

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, such as the proposed JOLT Act of 2012, to expand VWP participation and to promote international travel and tourism to the United States while maintaining our strong commitment to security. Additionally, as part of the President's recent Executive Order, we are working with international partners to meet existing requirements and prepare for further expansion of the VWP.

Overstays and Exit Capabilities

Over the past year, we have worked to better detect and deter those who overstay their lawful period of admission through the enhanced biographic program. The ability to identify and sanction overstays is linked to our 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, as part of Phase 1 of the enhanced biographic effort, DHS began a coordinated effort to vet all potential overstay records against Intelligence Community and DHS holdings for national security and public safety concerns. 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.

Through limited automated means, DHS cross-referenced additional overstay leads with DHS location and immigration holdings, closing additional records by confirming changes in immigration information or travel history that had not yet been recorded. Previously, these records would not have been examined, except in instances when resources allowed it. Now, we are vetting all overstays for public safety and national security concerns, and DHS is also conducting automated reviews for changes in immigration status or travel history. This is performed on a recurrent basis.

In July, Congress approved DHS's plan to continue building its enhanced biographic capability. DHS is implementing Phase 2 of this effort, and expects to have these enhancements in place by early 2013. Once completed, this initiative will significantly strengthen 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 also enhance our ability to identify individual overstays; provide the State Department with information to support visa revocation, prohibit future VWP travel for those who overstay, 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.

Concurrently, S&T is working to establish criteria and promote research for emerging technologies that would provide the ability to capture biometrics and develop a biometric exit capability at a significantly lower operational cost than is currently available. S&T is collaborating with the National Institute of Standards and Technology (NIST) on this initiative.

Lastly, as part of the *Beyond the Border Action Plan* signed by President Obama and Canadian Prime Minister Harper in December 2011, we are creating an exit program on the United States northern border. Under the plan, the United States and Canada will exchange entry records, so that an entry to one country essentially becomes an exit record from the other.

Protecting Surface Transportation

Beyond aviation, we have worked with Federal agencies and other government partners, 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 must be 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 Baseline Assessments for Security Enhancement conducted in multiple modes of transportation on a continuous basis to elevate standards and identify security gaps.

We continue to support surface transportation security through the deployment of 37 Visible Intermodal Prevention and Response (VIPR) teams, which include 12 multi-modal teams added in FY 2012. 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 detect, deter, and prevent potential terrorist acts and disrupt pre-operational surveillance or planning activities.

These efforts have been supported by grant funding 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.

We know that a crisis or vulnerability in any part of the world has the ability to impact the flow of goods and people thousands of miles away. Beyond loss of life and physical damage, these

events can cause large economic consequences. Therefore, our economy is dependent on our ability to secure and facilitate the flow of people and goods to and from our shores.

Within the American economy, trade with our international partners accounts for roughly one quarter of our GDP. This year alone, DHS will help facilitate about $2 trillion in legitimate trade, while enforcing U.S. trade laws that protect the economy, the health, and the safety of the American people.

Earlier this year, the Administration announced the U.S. National Strategy for Global Supply Chain Security to set a Government-wide vision of our goals, approach, and priorities to strengthen the global supply chain system. The National 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.

In addition to 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 in partnership with multilateral organizations such as the International Maritime Organization (IMO), the International Civil Aviation Organization (ICAO), the World Customs Organization (WCO), Universal Postal Union (UPU), and the Asia-Pacific Economic Cooperation (APEC) forum as well as bilaterally with trading partners.

Just last week in Montreal, I attended ICAO's ministerial conference on aviation security, where I met again with the Secretary General and counterpart ministers and reached an agreement regarding global air cargo security standards.

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.

Through the Container Security Initiative (CSI), CBP works with host government customs services to examine high-risk maritime containerized cargo at foreign seaports, before they are loaded on board vessels destined for the United States. CSI currently operates at a total of 58 ports in North America, Europe, Asia, Africa, the Middle East, and Latin and Central America—covering approximately 80 percent of all maritime containerized cargo imported into the United States. In addition, cargo that does not pass through a CSI port is screened at the National Targeting Center-Cargo and scanned by specialized CBP units located at the first port of arrival within the United States. Currently, CBP has 398 Radiation Portal Monitors (RPMs) at

priority seaports in the United States, through which approximately 99 percent of all containerized cargo volume passes.

S&T is also pursuing a number of innovative approaches to supply chain and cargo security, including maintaining maritime cargo and container integrity; tracking containers and conveyances; and, detecting and interdicting dangerous and illicit goods. Currently, S&T is piloting a land-based container and conveyance security pilot with our trading partners in Canada and Mexico. In FY 2013 we plan to expand the pilot program by conducting a maritime cargo and container security pilot with our EU colleagues.

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 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. We are also building partnerships, through mutual recognition arrangements, with foreign governments maintaining industry partnership programs compatible with CBP's Customs-Trade Partnership against Terrorism. We signed a Mutual Recognition Decision with the European Union in May which will strengthen international supply chain security and facilitate trade with the EU.

DHS is also focused on preventing the exploitation of the global supply chain by those seeking to use the system to transport dangerous, illicit cargo, contraband, contaminated or counterfeit products. For example, under Program Global Shield, we are working with more than 90 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 127 metric tons of these deadly materials.

DHS, through ICE and CBP, 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 ensuring that 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 FY 2011, ICE initiated 1,780 new investigations into illicit procurement activities, made 583 criminal arrests, and accounted for 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.

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.

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 (BEST), 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, in coordination 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 651 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 352 miles of pedestrian fence.

To enhance cooperation among local, tribal, territorial, state and Federal law enforcement agencies, we have provided more than $202 million in Operation Stonegarden funding to Southwest border law enforcement agencies over the past four years.

Our work along the border has included effective support from the Department of Defense (DOD).. In addition to continuing support from DOD's Joint Interagency Task Force (JIATF)-North, 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 deployment of border surveillance technology and equipment that will strengthen our ability to identify and interdict the smuggling of people, drugs, illegal weapons, and money.

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 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. And this year, CBP introduced an extremely effective new aviation surveillance technology to monitor the border. The U.S. Army has loaned CBP a new electronic sensor system. CBP flies Predator B unmanned aircraft systems (UASs) with this new system on the Southwest border. This system provides DHS with the first broad area, electronic sensor system, with capabilities that far exceed those of the ground based fixed or mobile systems.

The results of these comprehensive and coordinated efforts have been significant. Border Patrol apprehensions—a key indicator of illegal immigration—have decreased 53 percent in the last three years and have decreased 80 percent from 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 according to FBI Uniform Crime Report data, and statistics have shown that some of the safest communities in America are along the border. From FYs 2009 to 2011, DHS seized 74 percent more currency, 41 percent more drugs, and 159 percent more weapons along the Southwest border as compared to FYs 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 FYs 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.

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 FY 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 FY 2010.

Northern Border

To protect the Northern border, we have continued to deploy technology and resources, invest in port of entry improvements to enhance security, and deepen our 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 opened the Operations Integration Center in Detroit—a multi-agency communications center for DHS, and other Federal, state, local, and Canadian law enforcement agencies. The Operations Integration Center increases information sharing capabilities leading to seizures of drugs, money, and illegal contraband along the northern border within the Detroit Sector.

ICE has four BEST units along the northern border. These units, including representatives from the Royal Canadian Mounted Police, Canadian Border Services Agency and numerous other provincial Canadian police departments, enhance coordination of U.S.-Canada joint interdictions and investigations, resulting in increased security for both countries.

Recognizing the continued importance of the U.S.-Canada partnership, President Barack Obama and Canadian Prime Minister Stephen Harper released the joint declaration, *Beyond the Border: A Shared Vision for Perimeter Security and Economic Competitiveness*, on February 4, 2011. This declaration committed the United States and Canada to pursue a perimeter approach to security, working together within, at, and away from the borders of our two countries to enhance our security and accelerate the legitimate flow of people, goods, and services between our two countries. *Beyond the Border* includes multiple Cabinet-level departments, reflecting a true interagency effort within each government and in a bi-national capacity.

Our countries have committed to improving information sharing while respecting each country's respective constitutional and legal frameworks. Specific examples of information sharing initiatives under the *Beyond the Border Action Plan* include efforts to:

- Share risk assessment/targeting scenarios, and enhance real time notifications regarding the arrival of individuals on U.S. security watchlists;
- Provide access to information on persons who have been removed or who have been refused admission or a visa from either country, as well as those who have been removed from their respective countries for criminal reasons; and
- Implement a systematic and automated biographic information sharing capability by 2013 and biometric information sharing capability by 2014 to reduce identity fraud and enhance screening decisions, and in support of other administrative and enforcement actions.

Together, these initiatives will help improve immigration and border processes and decision making, establish and verify the identities of travelers, and permit screening to be conducted at the earliest point possible.

To support the *Beyond the Border Action Plan*, in June we released the DHS Northern Border Strategy, the first unified strategy to guide the department's policies and operations along the U.S.-Canada border. Through this strategy, we will continue to work to improve information sharing and analysis within DHS, as well as with our partners. We will enhance coordination of U.S.-Canada joint interdictions and investigations, deploy technologies to aid joint security efforts along the border, and continue to update infrastructure to facilitate travel and trade. We also look forward to continuing to deepen partnerships with Federal, state, local, tribal, private sector, and Canadian partners that are so critical to the security, resiliency, and management of our Northern border.

Maritime

With more than 350 ports and 95,000 miles of coastline, the U.S. maritime domain is unique in its scope and diversity.

The Coast Guard provides maritime security using a major cutter and patrol boat fleet to respond to threats, and launch boats and aircraft to maintain a vigilant presence over the seas. Closer to shore, Coast Guard helicopters small cutters and boats monitor, track, interdict, and board vessels. In the Nation's ports, the Coast Guard and CBP, along with our Federal, state, local, and tribal partners, working in concert with other port stakeholders, monitor critical infrastructure, conduct vessel escorts and patrols, and inspects vessels and facilities.

The U.S. Coast Guard plays an integral role in DHS's border enforcement strategy through its maritime operations as part of JIATF-South, the U.S. Southern Command entity that coordinates integrated interagency counter drug operations in the Caribbean Sea, Gulf of Mexico, and the eastern Pacific. In FY 2011, Coast Guard major cutters and other assets removed over 75 metric tons of cocaine, more than 17 metric tons of marijuana, detained 191 suspected smugglers, and seized 40 vessels. Additionally, Coast Guard Law Enforcement Detachments are deployed aboard U.S. Navy and Allied assets to support detection, monitoring, interdiction and apprehension operations. CBP Office of Air and Marine P-3 and Coast Guard fixed-wing aircraft have also been an integral part of successful counter-narcotic missions operating in the Source and Transit Zones in coordination with JIATF-South. Collectively the efforts to interdict drugs in the Source and Transit Zones helped to control the flow of drugs to the Southwest border.

Robust interagency cooperation and strong international partnerships also helped the Coast Guard interdict 2,474 migrants at sea in FY 2011.

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. While we are more network dependent than ever before, increased interconnectivity increases the risk of theft, fraud, and abuse.

Cyber incidents have increased significantly over the last decade and the United States continues to confront a dangerous combination of known and unknown vulnerabilities in cyberspace, strong and rapidly expanding adversary capabilities, and limited threat and vulnerability awareness. There have been instances of theft and compromise of sensitive information from both government and private sector networks. 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.

DHS is the Federal government's lead agency for securing civilian government computer systems and works with our industry and Federal, 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. DHS also 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.

With respect to critical infrastructure, DHS and the sector specific agencies work together 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. Protecting critical infrastructure requires taking an integrated approach toward physical and cyber security and ensuring that we can utilize our established partnerships with the private sector to address cyber security concerns. 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.

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. DHS, in collaboration with the Department of State and other departments/agencies, also works with international partners on cyber threats and other cybersecurity issues, as appropriate.

To combat cyber crime, DHS leverages the skills and resources of the U.S. Secret Service (USSS) and ICE, who investigate cyber criminals and work with the Department of Justice, which prosecutes them. Within DHS, cyber crime investigations are directly led by the USSS

and involve numerous partners at the Federal, state and local level as well as the private sector. In FY 2011 alone, USSS prevented $1.6 billion in potential losses through cyber crime investigations. Additionally, ICE HSI cyber crime investigations relating to child exploitation in FY 2011 resulted in 1,460 criminal arrests, 1,104 indictments and 928 convictions. One significant child exploitation investigation conducted by ICE HSI was Operation Delego, which resulted 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 child pornography. To date, 43 of these individuals have been convicted.

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.

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, and 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 FY 2012. We are currently working with the Defense Industrial Base to exchange actionable information about malicious activity.

As much as we are doing, we must do even more. All sides agree that Federal and private networks must be better protected, and information about cybersecurity threats must be shared more easily while ensuring that privacy and civil liberties are protected through a customized framework of information handling policies and oversight. DHS is committed to ensuring cyberspace supports a secure and resilient infrastructure, enables innovation and prosperity, and protects privacy and other civil liberties by design.

The Administration sent Congress a legislative package in May 2011 that included the new tools needed by homeland security, law enforcement, intelligence, military and private sector professionals to secure the Nation, while including essential safeguards to preserve the privacy rights and civil liberties of citizens. Since that time, Administration officials have testified at 17 hearings on cybersecurity legislation and presented over 100 briefings, including two all-Member Senate briefings and one all-Member House briefing.

The *Cybersecurity Act of 2012* would have begun to address vulnerabilities in the Nation's critical infrastructure systems. This legislation was the result of years of work. It reflected input from the Administration, the private sector, privacy experts, and Members of Congress from both sides of the aisle. Numerous current and former homeland and national security officials had also expressed the importance and urgency of this legislation.

The American people expect us to secure the country from the growing danger of cyber threats and ensure the Nation's critical infrastructure is protected. The threats to our cybersecurity are real, they are serious, and they are urgent. We will continue to work with the Congress – and this Committee – to pass strong cybersecurity legislation to give DHS and our partners the tools

and authorities we need to continue to protect cyberspace while also protecting privacy and civil rights.

Ensuring Robust Privacy and Civil Rights and Civil Liberties Safeguards

The Department builds privacy and civil rights and civil liberties protections into its operations, policies, programs, and technology deployments from the outset of their development.

The DHS Privacy Office – the first statutorily required privacy office of any Federal agency – partners with every DHS component to assess policies, programs, systems, technologies, and rulemakings for privacy risks, and recommends privacy protections and methods for handling personally identifiable information. To further integrate privacy and reinforce the headquarters privacy office, a team of privacy officers are embedded into the operational components throughout the Department.

DHS's Office for Civil Rights and Civil Liberties plays a key role in the Department's mission to secure the Nation while preserving individual freedoms and represents the Department's commitment to the idea that core civil rights values—liberty, fairness, and equality under the law—are a vital part of America, and that these values provide a bulwark against those who threaten our safety and security.

Since its inception, CRCL has expanded its participation in programs and activities throughout the Department and continued its efforts to promote civil rights and civil liberties. For example, CRCL collaborates with ICE on detention reform and other immigration-related efforts, and works with TSA to ensure that evolving aviation security measures are respectful of civil rights and civil liberties.

CRCL's community engagement efforts include a wide variety of stakeholders and organizations through regular roundtables and other tools across the country. CRCL has also expanded its training capacity and worked closely with the DHS Privacy Office and the Office of Intelligence and Analysis to offer civil rights and civil liberties training for fusion centers, as well as training to a number of the Department's Federal, state, and local partners.

Conclusion

While America is stronger and more resilient as a result of these efforts, threats from terrorism persist and continue to evolve. Today's threats do not come from any one individual or group. They may originate in distant lands or local neighborhoods. They may be as simple as a homemade bomb or as sophisticated as a biological threat or coordinated cyber attack.

As threats to our Nation evolve, DHS must also evolve. Thus, we continue to remain vigilant, protecting our communities from terrorist threats, while promoting the movement of goods and people and maintaining our commitment to civil rights and civil 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.