Statement for the Record

Acting Secretary Rand Beers

U.S. Department of Homeland Security

Before the

United States Senate

Committee on Homeland Security and Governmental Affairs

November 14, 2013

Introduction

Thank you, Chairman Carper, Ranking Member Coburn, and Members of the Committee. I appreciate the opportunity to appear before the committee to discuss the Department of Homeland Security's (DHS) efforts to prepare for, protect against, respond to and recover from threats facing our nation and the American people.

At the outset, I want to thank Federal Bureau of Investigation (FBI) Director James Comey and National Counterterrorism Center (NCTC) Director Matthew Olsen for their strong collaboration as together we work to meet the shared responsibility of keeping our nation safe. I also want to thank Congress for your guidance and support over the past four years, and indeed, since the Department's founding ten years ago.

In addition, I would like to urge Congress to swiftly confirm Jeh Johnson, President Obama's nominee to be our nation's next Secretary of Homeland Security. I have known Jeh for a long time. He cares deeply about the mission of this department and will bring considerable skill, intellect, experience, and dedication to our nation's efforts to address evolving threats. In short, he will be an excellent Homeland Security Secretary.

Let me also say at the outset that the entire DHS family continues to mourn the loss of Transportation Security Officer Gerardo Hernandez, who was killed in the shooting at Los Angeles International Airport on November 1st.

As you know, Officer Hernandez was the first TSA officer killed in the line of duty. This senseless act of violence reminds us of the dangers our men and women on the frontlines face every day, and the very real sacrifices they often make on our behalf. We continue to work closely with the FBI and our state and local law enforcement partners to fully investigate this crime and ensure justice is served. As always, our security posture, which at all times includes a number of measures both seen and unseen, will continue to respond appropriately to protect the American people.

Of course, DHS relies on many partners from across our nation to meet our diverse missions. In this way, homeland security is not the charge of a single department or agency, but the responsibility of all of us, from our largest city police force to smallest law enforcement jurisdiction, our biggest company to smallest independent business, from the Whole Community to each individual within those communities.

This "homeland security enterprise" is integral to our nation's ability to address threats in a timely and comprehensive fashion. For this reason, DHS has worked with partners all across our country to build critical capabilities at the state, local, tribal, and territorial levels, share information, protect infrastructure in partnership with the private sector, enhance preparedness and resilience, and address new and evolving threats, such as those in cyberspace.

Since DHS's creation ten years ago, our country is stronger, better equipped to handle threats, and more nimble in our ability to respond and recover. Our progress is a testament to the hard work of more than 240,000 DHS employees and our strong partnerships with Federal, state, and

local officials, including law enforcement and emergency managers, non-profit and faith-based organizations, and an engaged and vigilant public.

Nevertheless, we know threats to the homeland continue to evolve. As we have seen in recent months with the Boston Marathon attacks, we face a dynamic threat environment that includes threats from abroad as well as those that originate within our borders. These threats can come from international terrorist organizations, groups inspired by terrorist ideology but with no operational connections to core groups or affiliates, as well as lone wolves, often with no particular ideological motivation, yet still intent on doing widespread harm.

Within the context of U.S.-based violent extremism, we know that al-Qa'ida, its affiliates, and allies use propaganda to inspire prospective U.S.-based supporters to conduct terrorist attacks in the West and especially the homeland. Lone offenders – prime targets of al-Qa'ida's English-language messaging, such as the online magazine Inspire – tend to favor plots involving the use of easily acquired weapons against local targets. These lone offender plots are especially challenging because they can be tactically simple and adaptable, complicating disruption by authorities.

However, although we are concerned about the threat posed by al-Qa'ida or individuals inspired by al-Qa'ida, the threat posed by violent extremists is a broader threat not limited to a single ideology. Because the threat environment constantly evolves, DHS must consider all types of violent extremism, while ensuring we do not inappropriately focus upon individuals who may be engaging in legal, constitutionally-protected behavior, such as political speech. To this end, DHS focuses its attention on individuals who are inspired not merely by specific ideologies, but are inspired to violence and/or specific criminal activity as a means of furthering their ideological objectives. Many communities and rural counties nationwide face such threats.

Lone offenders and small groups of individuals are one of the greatest and most difficult threats to counter. In recent years, we have observed several acts of violence by lone offenders against military targets, as well as attempted attacks targeting civilian populations by individuals inspired by extremist ideology. Domestic terrorism, and those individuals not inspired by foreign terrorist groups, remains a persistent threat.

Today I will discuss how DHS works with our partners to address these and other threats, building on our work over the past ten years while implementing new programs and initiatives to ensure we remain agile and adaptable, learn and apply lessons from past attacks, and continue to protect individual liberties and privacy while supporting our economy.

Guarding Against Terrorism

Guarding against terrorism is the founding mission of DHS. While this is not our only mission, it has been our primary focus since our inception. DHS recognizes that we cannot prevent all threats all the time, nor can we guarantee the safety of every community against all hazards. Our chief operating principle, therefore, has been to work with partners at all levels to enhance our collective ability to detect and deter high-risk threats as early as possible, build capabilities to respond to them when required, and enhance our ability to quickly recover after the fact.

Building State and Local Capacity

DHS has worked to get information, tools, and resources into the hands of state, local, tribal, and territorial officials. We have done so by focusing on four key priorities: (1) improving the sharing of both classified and unclassified information regarding potential threats to the homeland; (2) building grassroots analytic capabilities at the state and local levels; (3) standardizing how we train state, local, tribal, and territorial law enforcement to recognize behaviors and indicators that have historically been associated with terrorism and report suspicious activities; and (4) increasing community awareness and encouraging the public to report suspicious activity to law enforcement.

A cornerstone of this effort has been our support for state and major urban area fusion centers. To date, DHS has deployed 96 Office of Intelligence and Analysis (I&A) personnel to fusion centers throughout the country to coordinate with intelligence and law enforcement personnel. We also have deployed 71 Homeland Secure Data Network (HSDN) systems across the country to provide access to Secret information and intelligence.

Moreover, we have trained state and local analysts at fusion centers to ensure they have the necessary skills and expertise to analyze and place intelligence and information from the Intelligence Community within local and regional contexts to produce relevant and timely products. And we have developed tailored products to meet the needs of our state and local partners and expanded distribution to ensure relevant and appropriate information is shared with those who need it.

Providing Training and Resources

We provide support through a variety of training and exercises to our law enforcement and community partners. DHS has worked closely with the FBI on the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) to ensure frontline law enforcement receive training in how to appropriately report suspicious activity while protecting individual rights and liberties.

We have worked with the Department of Justice (DOJ), including the FBI, and NCTC on Countering Violent Extremism (CVE) training and outreach, with three primary goals. First, we are working to better understand the phenomenon of violent extremism through extensive analysis and research on the behaviors and indicators associated with violent extremism. Second, we are addressing the dynamics of violent extremism by strengthening our partnerships with a broad and diverse range of domestic and international partners from state and local governments and law enforcement, to faith-based organizations and community groups.

Since 2011we have worked with law enforcement partners to develop CVE training to ensure frontline law enforcement officers understand behaviors potentially indicative of violent extremist activity. As part of this effort, we recently launched a joint DHS/DOJ-FBI web-based portal that contains training materials for law enforcement and first responder training practitioners, as well as hundreds of additional tools and resources for countering the threats from violent extremism, terrorist activity, and mass casualty attacks.

We are leveraging our resources to help law enforcement and the private sector to address active shooter situations. For example, we have hosted Active Shooter Workshops and training sessions for law enforcement to discuss lessons learned from past active shooter situations and best practices. Working with commercial facilities, we developed training to better prepare store managers and hourly personnel to respond to a potential active shooter incident. We also created a new active shooter page on the DHS website – www.dhs.gov/active-shooter-preparedness – with resources designed for law enforcement as well as the public on how to respond to active shooter incidents.

The Federal Law Enforcement Training Center (FLETC) offers active shooter training and resources to numerous law enforcement agencies at the federal, state, local, tribal, and territorial levels. FLETC also collaborates with partners at DOJ and in academia to take a holistic approach to developing strategies aimed at preventing incidents of multiple casualty violence. Bringing together subject matter experts from a cross-section of pertinent disciplines, including law enforcement, academia, law, health administration, medicine, private security, and education, FLETC hosted two summits during Fiscal Year 2013 to further the national dialogue on preventing multiple casualty violence, specifically addressing concepts such as information-sharing across jurisdictions and community-based prevention models.

The DHS Office of Health Affairs is working with other Federal agencies to develop Federal guidance for fire, EMS, and law enforcement on the medical response to Improvised Explosive Device (IED) and Mass Shooting incidents. DHS is planning interagency engagements with fire, EMS, and law enforcement stakeholders over the next six months on this issue.

The Federal Protective Service (FPS) provides coordination and assistance to Federal agency officials on Occupant Emergency Plan (OEP) development. These plans are intended to minimize risk to personnel, property, and other assets within a Federal facility by providing a facility-specific response plan and evacuation procedures for occupants. FPS also provides agency-specific evacuation training and drills which incorporate work place violence and active shooter awareness training.

Because an engaged and vigilant public is vital to our efforts to protect our communities, DHS has continued expansion of the "If You See Something, Say Something™," campaign to more than 250 states, cities, transportation systems, universities, and private sector entities nationwide to encourage the public to play an active role in reporting suspicious activity.

Building Capabilities to Counter Improvised Explosive Devices (IEDs)

Through the Office for Bombing Prevention (OBP), DHS partners with both public and private sector partners to build capabilities to prevent, protect against, respond to, and mitigate bombing incidents such as the Boston Marathon attack. OBP conducts Bombing Prevention training and Multi-Jurisdiction IED Security Planning workshops to assist with the development of IED security plans to integrate assets and capabilities from multiple areas and emergency service sectors in responding to an IED attack. The workshop and plan development is a systematic

process that fuses counter-IED education, capability analysis, training, and planning tailored to the unique requirements of high-risk jurisdictions.

OBP hosts the Bomb-making Materials Awareness Program (BMAP), a joint OBP-FBI program that promotes private sector, point-of-sale awareness, and SAR training to prevent misuse of dual-use explosive precursor chemicals and components commonly used in IEDs. BMAP cultivates prevention opportunities by building a network of aware and vigilant private sector partners who serve as the Nation's counter-IED "eyes-and-ears."

OBP maintains TRIPwire, an online, information-sharing network for bomb squad, law enforcement, and other emergency services personnel. TRIPwire shares critical information with public and private sector partners during periods of heightened alert or following IED-related incidents. Following the Boston Marathon attack, for example, use of TRIPwire increased to nearly 600,000 hits alone on April 16th.

The Administration is undertaking efforts to enhance counter- IED prevention, protection, response, and mitigation. DHS is supporting programmatic coordination and implementation of the National Policy for Countering IEDs, and with our interagency partners we are working across the Federal government to ensure programs are being properly integrated and leverage the knowledge and resources available to ensure public and private sector partners have the capabilities to counter IED-related threats.

Boston Marathon Response

The results of our efforts are communities across the United States that are better equipped to handle a variety of threats, including terrorism. We need only look at the timely and well-coordinated response to the despicable Boston Marathon attack to see how investments in building state and local capacity contributed to an effective, integrated response by the Boston community – one that ultimately prevented more lives from being lost on that horrible day.

In previous years, DHS provided homeland security grants to the City of Boston and Commonwealth of Massachusetts to equip and train special response teams in improvised explosive device detection, prevention, response, and recovery. We supported more than a dozen exercises in Boston, including one that focused on a large, mass-casualty event and involved hundreds of responders last November. And we supported the creation of the Medical Intelligence Center to enable information sharing across the Boston medical community.

The President declared a state of emergency on April 17, allowing the Federal Emergency Management Agency (FEMA) to coordinate the provision of emergency protective measures in response to the attack. The well-executed emergency response that immediately followed the Boston Marathon attack was the product of years of planning, training, and investment in building state and local capacity. Without the selfless service of so many heroic individuals and first responders, the toll from this attack could have been far greater, and this terrible tragedy could have been even worse. Already DHS has brought together law enforcement, first responders, and others involved to examine the response and identify lessons that we may apply in the future to prevent such attacks and ensure an effective response if they occur.

Enhancing Inbound Targeting of Passengers and Cargo

As this committee knows well, threats from abroad, in particular those directed at our aviation system, have continued to evolve over the past decade. In addition to the attempted terrorist attack against Northwest Airlines Flight #253 on Christmas Day in 2009, we have seen the attempted bombings of cargo planes bound from Yemen in 2010. Last year, the international community also thwarted a plot that would have targeted a U.S-bound airliner with explosives.

Al-Qa'ida in the Arabian Peninsula (AQAP) remain the Al-Qa'ida affiliate about which we have the greatest concern because of its demonstrated and continuing interest in advancing plots to attack the homeland, particularly the aviation industry. We remain concerned that AQAP continue to seek ways to circumvent existing security measures, using tactics that are creative and increasingly sophisticated. Despite the death of Anwar al-Aulaqi, the group's master bomb maker and other key leaders remain alive, and the group almost certainly maintains the intent and capability to attack the homeland with little to no warning.

We have responded to such threats comprehensively and in a manner that underscores the international scope of the aviation system. Shortly after the 2009 Christmas Day plot, DHS launched a major international initiative to address existing security vulnerabilities in aviation. In 2010 the International Civil Aviation Organization (ICAO) General Assembly unanimously supported a historic new Declaration on Aviation Security. This Declaration provided a unified vision for strengthening security in the areas of information collection and analysis, information sharing and passenger vetting, the development of security standards, and deployment of technology.

Since that time, governments and aviation industry partners have worked to meet the objectives of the Declaration, including adapting to new and emerging threats, and addressing them swiftly and decisively; and raising the level of security through assistance and capacity development. As of January of this year, 19 countries have deployed or piloted Advanced Imaging Technology (AIT) in their major airports to screen passengers for metallic and non-metallic threats, including weapons, explosives, and other objects concealed under layers of clothing. In addition, the Transportation Security Administration (TSA) now has agreements with 64 foreign governments permitting Federal Air Marshals to be present on international U.S. carrier flights.

Importantly, we have continued to build a layered approach to aviation security that includes the prescreening of passengers; the deployment of new technologies; training of airport security and law enforcement personnel to better detect behaviors potentially associated with terrorism; and strengthening of air cargo security. We are integrating this risk-based, intelligence driven approach into everything we do to identify passengers and cargo that warrant additional scrutiny, providing the most effective transportation security in the most efficient way possible.

To become more risk-based, we have sought to leverage information to identify threats earlier and share that information with our foreign counterparts and aviation sector partners. In April of 2012, the United States ratified a new agreement with the European Union to continue the transfer of Advance Passenger Information/Passenger Name Records (API/PNR), an important

milestone in our collective efforts to protect the international aviation system from terrorism and other threats. Analysis of API/PNR data allows us to better identify passengers we should pay more attention to before they arrive at the airport.

We also leverage information to enhance our inbound targeting operations through programs like the Pre-Departure Targeting Program and Immigration Advisory Program (IAP), which help identify high-risk travelers likely to be inadmissible to the U.S., and make recommendations to commercial carriers to deny boarding. From Fiscal Year 2010 to 2012, U.S. Customs and Border Protection (CBP) worked with our partners in the airline industry to prevent 8,984 high risk travelers from boarding aircraft to the United States as a result of its Pre-Departure and Immigration Advisory/Joint Security Programs.

CBP also operates preclearance operations at 15 locations in five countries, allowing for the complete security screening and formal determination of admissibility of travelers to the United States before they board a U.S-bound flight. In Fiscal Year 2012, CBP processed 15.6 million travelers through preclearance operations.

Through the Visa Security Program, U.S. Immigration and Customs Enforcement (ICE) also has deployed agents to high-risk visa activity posts overseas to identify potential terrorist and criminal threats before those individuals are granted a U.S. visa. And to further enhance visa-screening efforts, ICE, CBP and the Department of State (DOS) are collaborating on an automated visa application screening process that broadens the scope for identifying potential derogatory information prior to visa adjudication and issuance, and synchronizes reviews of the information across these agencies. Since the program's inception in January 2013, more than 1.9 million visa applications have been received and 1,304 have been returned to DOS for disapproval, including 950 for security-related reasons.

Air Cargo Security

With respect to air cargo security, DHS has worked with partners around the world to recognize National Cargo Security Programs (NCSPs) that further strengthen international air cargo security. As of September 2013, TSA has recognized the programs of 37 countries, which account for approximately 67 percent of inbound cargo to the United States on passenger aircraft.

We are also formalizing and expanding our Air Cargo Advance Screening (ACAS) pilot, a joint effort between TSA and CBP that enables members of the air cargo industry to send and receive advance security filing data for their air cargo, which helps us identify high-risk shipments for enhanced screening. As of September 2013, there are 81 entities participating in the ACAS pilot and over 100 million shipments have been successfully processed.

Moreover, today 100 percent of all air cargo on passenger aircraft that depart U.S. airports, or airports which serve as the last point of departure to the U.S., is screened to provide a level of security that is commensurate with the level provided by screening of passenger checked baggage. TSA Transportation Security Specialists (TSSs) verify compliance with security requirements, including screening, for all air carriers which operate into the United States.

More broadly, DHS continues to work with international organizations such as ICAO, World Customs Organization (WCO), and Universal Postal Union (UPU) to develop broad air cargo and mail security guidelines and standards. This strategy is designed to enlist other nations, international bodies, and the private sector in increasing the security of the global supply chain by adopting new inbound cargo targeting rules, institutionalizing a supply chain approach to security, implementing additional and enhanced screening for all cargo identified as high risk, and improving sharing of advanced cargo data and electronic shipping information.

Facilitating Trade and Travel

While these measures are important, we have not forgotten our imperative to facilitate lawful trade and travel to and from the United States. Accordingly, DHS has focused on leveraging information and technology to expedite legitimate travelers consistent with our risk-based approach. TSA has implemented various measures to focus its resources and improve the passenger experience at security checkpoints by applying intelligence-driven, risk-based screening procedures and enhancing its use of technology, including deployment of AIT machines to nearly 160 airports nationwide.

We also have expanded popular and successful trusted traveler programs such as Global Entry and TSA Pre✓™. Global Entry expedites pre-approved, low risk air travelers entering the United States, in many cases allowing them to clear customs and immigration processing within minutes. Similarly, TSA Pre✓™ provides expedited screening for airline travelers.To date, more than 18 million travelers have experienced TSA Pre✓™ at 100 airports nationwide.

In July, TSA also announced a new process that will allow even more U.S. citizens and Lawful Permanent Residents to enroll in TSA Pre✓™ by enabling them to apply online and visit an enrollment site to provide identification and fingerprints. TSA also offers expedited screening to more low-risk travelers by using information already provided by passengers through its existing Secure Flight program requirements. This process allows TSA to maintain its high security standards and create greater efficiency while offering more travelers the benefit of expedited screening through TSA Pre✓™ lanes.

And with respect to the facilitation of cargo, we have continued to strengthen and expand the Customs-Trade Partnership Against Terrorism (C-TPAT), our trusted shipper program that provides validated members with expedited customs processing.

Enhancing Border Security and Combating Transnational Crime

Of course, effective border security is essential to a safe, secure homeland. Over the past four and a half years, DHS has invested historic resources to protect our borders and prevent illegal cross-border activity. Because of these investments in manpower, technology, and infrastructure, our borders are now better staffed and protected than any time in our nation's history.

We have doubled the number of Border Patrol agents from approximately 10,000 in 2004 to more than 21,000 agents today. We have reinforced law enforcement capabilities at the ports of entry, increasing our numbers of CBP personnel from 17,279 customs and immigration inspectors in 2003, to more than 21,000 officers and 2,400 agriculture specialists today.

Supplementing this increase in personnel, we have made unprecedented investments in border infrastructure and technology, including the deployment of integrated fixed towers, mobile surveillance units, and thermal imaging systems along the borders, as well as new technology at the ports of entry, including Non-Intrusive Inspection and Radiation Portal Monitor technology to identify contraband and weapons of mass effect. We have expanded aerial coverage of the border as well, including Unmanned Aerial Systems that now cover the entire Southwest border from California to Texas, and 950 miles along our Northern border, providing critical aerial surveillance assistance to personnel on the ground.

CBP is also working closely with the DHS Science & Technology Directorate (S&T) to identify and develop technologies to improve our surveillance and detection capabilities on our land and maritime borders. This includes investments in tunnel detection and tunnel activity monitoring technology, low-flying aircraft detection and tracking systems, maritime data integration/data sharing capabilities, supply chain cargo security, and improved border surveillance tools.

We also have made our ports of entry more efficient through investments in technology and new requirements for secure travel documents as part of the Western Hemisphere Travel Initiative (WHTI). To date, more than 19 million individuals have obtained Radio Frequency Identification (RFID) technology-enabled secure travel documents that can be verified electronically in real-time to establish identity and citizenship and have reduced average vehicle processing times by 20 percent. CBP also conducts active lane management at land border ports as conditions warrant to accommodate trusted travelers and those with RFID-enabled documents.

By every traditional measure, this deployment of personnel, technology, and resources has led to unprecedented results. In addition to the historic lows in illegal alien apprehensions achieved over the past four years – down 50 percent from Fiscal Year 2008 – we have increased seizures of illegal drugs, weapons, and contraband. From Fiscal Years 2009 to 2012, CBP seized 71 percent more currency, 39 percent more drugs, and 189 percent more weapons along the Southwest border as compared to Fiscal Years 2006 to 2008.

Nationwide, CBP officers and agents also seized more than 4.2 million pounds of narcotics and more than $100 million in unreported currency through targeted enforcement operations. At U.S. ports of entry, CBP also arrested nearly 7,900 people wanted for serious crimes, including murder, rape, assault and robbery in FY 2012.

Additionally, in Fiscal Year 2012, Border Enforcement Security Task Forces (BESTs) made 2,812 criminal arrests, 853 administrative arrests, and federal prosecutors obtained 1,879 indictments and 1,671 convictions in BEST-investigated cases. BESTs consist of more than 1,000 members who represent more than 100 Federal, state, tribal, territorial, and international law enforcement agencies who have jointly committed to investigate transnational criminal activity along the Southwest and Northern borders and at our nation’s major seaports.

Along our maritime borders, the United States Coast Guard (USCG) actively contributes to our successful border security efforts. In Fiscal Year 2012, USCG seized over 107 metric tons of cocaine and 56 metric tons of marijuana destined for the United States; seized 70 drug trafficking vessels, detained 352 suspected smugglers; conducted over 11,600 annual inspections of U.S. flagged vessels; and conducted more than 9,000 Port State Control and Security examinations on foreign flagged vessels

Through prioritized enforcement investigations and operations, ICE Enforcement Removal Operations also removed record numbers of criminals from the United States while increasing its efforts to combat transnational criminal activity. In Fiscal Year 2012, approximately 55 percent, or more than 225,000, of the individuals that ICE removed from the United States were convicted of felonies or misdemeanors — a more than 96 percent increase since Fiscal Year 2008. Overall, 96 percent of ICE's removals fell into one of its priority categories of national security or public safety threats, repeat immigration violators, or recent border crossers. ICE also achieved significant success in its efforts to combat Transnational Criminal Organizations (TCOs). Since Fiscal Year 2011, ICE has disrupted or dismantled 285 of the most dangerous TCOs and individuals.

With respect to its counterterrorism mission, ICE-Homeland Security Investigations (HSI) remains DHS's largest partner in FBI Joint Terrorism Task Forces (JTTFs), where ICE-HSI special agents serve as leads or co-case agents on counterterrorism investigations where ICE's unique immigration or trade authorities are viewed as the most likely avenue to deter, disrupt or dismantle terrorist networks or terrorist attacks against the homeland.

In Fiscal Year 2012, ICE-HSI special agents assigned to JTTFs initiated 614 counterterrorism investigations, 129 of which focused specifically on charges for material support to terrorism. ICE HSI special agents arrested 532 subjects of investigations for various administrative or criminal charges including material support to terrorism, import/export violations, benefit fraud, financial fraud and violations of the Immigration and Nationality Act.

Protecting Critical Infrastructure and Cyber Networks

DHS coordinates the overall Federal effort to promote the security and resilience of the Nation's critical infrastructure. Working with the Sector-Specific Agencies established in PPD-21, DHS supports critical infrastructure owners and operators in preparing for, protecting against, mitigating from, responding to, and recovering from all-hazards events, including cyber incidents, terrorist attacks, and natural disasters. These activities promote the safety and security of the American public and ensure the provision of essential services and functions, such as energy and communications. To achieve this goal, DHS works with a variety of public and private partners to identify and promote effective solutions for security and resilience that address the risks facing the nation's critical infrastructure.

One lesson we have learned over the years is the need to work directly with stakeholders to enhance security and resilience of infrastructure. To this end, DHS has strategically deployed Protective Security Advisors across the United States to provide public and private sector

stakeholders with access to steady-state DHS risk-mitigation tools, products, and services, such as training and voluntary vulnerability assessment programs, in addition to supporting officials responsible for planning and leading National Special Security Events (NSSE) and Special Event Assessment Rating (SEAR) events. Protective Security Advisors support the response to all hazard incidents through field level coordination and information sharing, and provide expertise on reconstituting affected critical infrastructure.

Through the Protective Security Advisors, DHS also conducts onsite risk assessments of critical infrastructure and shares risk and threat information with state, local and private sector partners. In addition to helping owners and operators become more aware of the risks, hazards, and mitigation strategies, we are also helping them measure and compare their levels of security and resilience and how they can improve. In the last year, DHS conducted more than 900 vulnerability assessments and security surveys on critical infrastructure to identify potential gaps and provide the owners and operators with options to mitigate those gaps and strengthen security and resilience.

Cybersecurity

Our infrastructure protection efforts also include working closely with the private sector to protect our nation's information and communications technology against agile and sophisticated cyber threats. DHS is responsible for securing unclassified federal civilian government networks and working with owners and operators of critical infrastructure to help them secure their networks. We also coordinate the national response to significant cyber incidents and create and maintain a common operational picture for cyberspace across the government including building an integrated consequence analysis capability to evaluate critical infrastructure impacts from incidents, threats, and emerging risk.

This is critical, time-sensitive work, because we confront a dangerous combination of known and unknown cyber vulnerabilities, and adversaries with strong and rapidly expanding capabilities. Threats range from denial of service attacks, to theft of valuable trade secrets, to intrusions against government networks and systems that control critical infrastructure. These attacks come from every part of the globe, every minute of every day, and are continually increasing in seriousness and sophistication.

DHS Cyber Roles

Over the past four and a half years, cybersecurity has emerged as a top priority for DHS through our efforts to secure unclassified federal civilian government networks, work with critical infrastructure owners and operators, combat cyber crime, build a national capacity to promote responsible cyber behavior and cultivate the next generation of frontline cybersecurity professionals – all while keeping a steady focus on safeguarding the public's privacy, civil rights, and civil liberties.

To protect federal networks, DHS is deploying technology to detect and block cyber intrusions and developing continuous diagnostic capabilities, while providing guidance on what agencies need to do to protect themselves. For example, DHS deploys network intrusion detection and

prevention technology under a program known as Einstein. Through the Continuous Diagnostics and Mitigation (CDM) program, DHS is also taking a dynamic approach to fortifying the cybersecurity of computer networks and systems by providing capabilities and tools that enable network administrators to know the state of their respective networks at any given time, understand the relative risks and threats, and help system personnel to identify and mitigate flaws at near-network speed. When both programs are implemented, they will provide complementary protections across the "dot-gov" domain, further protecting the government's infrastructure and the nation's data.

DHS also works closely and regularly with owners and operators of critical infrastructure to strengthen their facilities through on-site risk assessment, mitigation, and incident response, and by sharing risk and threat information with the goal of strengthening the network defenses against outside attacks, maintaining system integrity, and preventing theft of proprietary information and trade secrets. For example, we provided classified cyber threat briefings and technical assistance to help banks improve their defensive capabilities following the recent series of denial of service attacks. DHS is also home to the National Cybersecurity & Communications Integration Center, an around-the-clock cyber situational awareness and incident response center that has responded to nearly 500,000 incident reports and released more than 26,000 actionable cybersecurity alerts to public and private sector partners over the past four years.

Last year, our U.S. Computer Emergency Readiness Team (US-CERT) also resolved approximately 190,000 cyber incidents and issued more than 7,450 alerts – a 68 percent increase from 2011. And our Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) responded to 177 incidents while completing 89 site visits and deploying 15 teams to respond to significant private sector cyber incidents.

Cybercrime

To combat cyber crime, DHS relies upon the skills and resources of USSS and ICE, and works with a variety of partner organizations and agencies to investigate cyber criminals. Since 2009, DHS has prevented $10 billion in potential losses through cyber crime investigations and arrested more than 5,000 individuals for their participation in cyber crime activities.

On July 25th, for example, DOJ announced the indictment of several individuals who directed a prolific criminal cyber hacking organization. USSS dismantled this transnational cybercrime ring after the group conspired in a worldwide hacking and data breach scheme that targeted major corporate networks and stole more than 160 million credit card numbers, which resulted in hundreds of millions of dollars in losses – the largest such scheme ever prosecuted in the United States. In Fiscal Year 2013, USSS cyber investigations accounted for over 1,000 arrests globally and prevented over $1.1 billion in fraud loss to U.S. financial institutions.

In 2001, Congress mandated USSS to establish a nationwide network of task forces to "prevent, detect and investigate various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems." Currently, USSS hosts 31 Electronic Crimes Task Forces (ECTF) that the Department leverages by combining the resources of academia, the private sector, and Federal, state and local law enforcement agencies.

USSS also collaborates with the State of Alabama to operate the National Computer Forensics Institute (NCFI), the nation's only federally-funded training center dedicated to instructing state and local officials in digital and cyber crime investigations. USSS opened the NCFI with a mandate to provide state and local law enforcement, legal and judicial professionals a free, comprehensive education on current cyber crime trends, investigative methods and prosecutorial challenges. Since its opening in 2008, the state-of-the-art facility has trained more than 2,400 state and local police officials, prosecutors, and judges from all 50 states and three U.S. territories. These NCFI graduates and members of the ECTFs represent over 1,000 state and local government agencies nationwide.

A recently executed partnership between ICE and USSS also will expand participation in the existing ECTFs to enhance their respective cyber investigative strengths, while maintaining their separate identities. And DHS is a partner in the National Cyber Investigative Joint Task Force, which serves as a collaborative entity that fosters information sharing across the interagency for investigating national security cyber threats.

Additional Collaboration and Coordination

At DHS, we have consistently stated that cybersecurity transcends national borders and requires operational collaboration, strategic dialogue, and an increased security and resilience of global supply chains. DHS works closely with the Department of State and our international partners to enhance information sharing, increase situational awareness, improve incident response capabilities, and coordinate strategic policy issues. DHS also works with international law enforcement partners to share expertise and resources to combat electronic crimes such as identity theft and intellectual property infringement, network intrusions, and a range of financial crimes.

For example, through the U.S.-EU Working Group on Cybersecurity and Cybercrime, DHS and our international counterparts develop collaborative approaches to a wide range of cybersecurity and cybercrime issues. ICE also works with international partners to seize and destroy counterfeit goods and disrupt websites that sell these goods. Since 2010, ICE and its partners have seized over 2,000 domain names associated with businesses selling counterfeit goods over the Internet. Additionally, USSS Cyber Operations Branch maintains an established collaboration of Cyber Working Groups with their international law enforcement partners in the Netherlands, the Baltic states, and Ukraine.

DHS also partners closely with the DOJ and Department of Defense to ensure that there is a whole of government approach with respect to responding to cyber incidents and threats. While each agency operates within the parameters of its authorities, our overall federal response to cyber incidents of consequence is coordinated among our three agencies. Where agency authorities overlap, as in law enforcement, protection, and response, we also directly coordinate with and support each other. This synchronization ensures that all of our capabilities are brought to bear against cyber threats and enhances our ability to share timely and actionable information with a variety of partners.

Science and Technology

DHS S&T supports a range of cyber security research and development efforts, targeting near-term and future capabilities that will carry through major improvements in cyber security of the homeland security enterprise.

For example, S&T contributed to protocols that help to protect Internet users from being covertly redirected to malicious websites, most critically including the Domain Name System Security Extensions technology, which helps prevent theft, fraud, and abuse online by blocking bogus page elements and flagging pages whose Domain Name System identity has been hijacked. S&T is also driving improvements through a Transition to Practice Program that will take some of the most promising federally funded cyber security technologies currently available and enable their transition into successful use.

S&T is also providing a key role in a multi-agency government wide effort directed by Executive Order (EO) 13636 on Improving Critical Infrastructure Cybersecurity and leading the Presidential Policy Directive (PPD) 21 on Critical Infrastructure Security and Resilience tasking to develop a national research and development plan for critical infrastructure security and resilience.

Recent Executive Actions

Cybersecurity remains a priority for the Administration, and while these accomplishments are significant, we need Congress to enact a suite of comprehensive cybersecurity legislation in order to be able to best meet this growing threat. We appreciate the efforts made in the last Congress to pass bipartisan cybersecurity legislation, but the inability to get this done has required the President to take executive action.

EO 13636 on Improving Critical Infrastructure Cybersecurity – issued in February of this year – supports more efficient sharing of real-time cyber threat information with the private sector. It also directs DHS to develop a voluntary program to promote the adoption of a new Cybersecurity Framework and assist the private sector in its implementation.

PPD 21 on Critical Infrastructure Security and Resilience directs the executive branch to strengthen our capability to understand and share information about how well critical infrastructure systems are functioning and the consequences of potential failures. And it calls for a comprehensive research and development plan to guide the government's effort to enhance market-based innovation.

These documents reflect input from stakeholders across government, industry, and the advocacy community. Furthermore, they help ensure that we protect individual privacy and civil liberties through transparent processes, additional stakeholder engagement – including consultation with the Privacy and Civil Liberties Oversight Board, privacy advocates and the public – and assessments releasable to Congress and the public by the privacy and civil liberties officials of the participating agencies in the cybersecurity programs envisioned by EO 13636 and PPD 21. Importantly, EO 13636 calls for us to work *within* current authorities and increase voluntary

cooperation with the private sector. It does *not* grant new regulatory authority or establish additional incentives for participation in a voluntary program.

In partnership with the Federal interagency, DHS established an Integrated Task Force to lead implementation of these executive actions. The task force has conducted more than 100 working sessions thus far and has already produced several deliverables. Among them are an Incentives Report that analyzes potential government incentives that could be used to promote the adoption of the Cybersecurity Framework, a description of critical infrastructure functional relationships, instructions on producing unclassified cyber threat reports to help critical infrastructure partners prevent and respond to significant threats, a method to identify and prioritize nationally and regionally significant cyber infrastructure assets, recommendations on incorporating security standards into acquisition planning and contract administration, and a process to expedite security clearances for the private sector.

Nevertheless, we continue to believe that a comprehensive suite of legislation is necessary to build stronger, more effective, public-private partnerships on cybersecurity. Specifically, Congress should enact legislation to:

- Incorporate privacy and civil liberties safeguards into all aspects of cybersecurity;
- Further increase information sharing, and establish and promote the adoption of standards for critical infrastructure;
- Give law enforcement additional tools to fight crime in the digital age; and
- Create a National Data Breach Reporting requirement.

DHS is committed to securing our nation from growing cyber threats and ensuring critical infrastructure is protected in partnership with the private sector, while safeguarding the public's privacy, civil rights, and civil liberties. We continue to urge Congress to take additional action to help us meet this important responsibility.

Conclusion

Chairman Carper, Ranking Member Coburn, and Members of the Committee: thank you for your steadfast partnership and support of DHS. Together, we have accomplished a tremendous amount to more effectively address the many threats facing the United States. But we know our work is not done and we must continue to be flexible and agile in a changing threat environment.

I look forward to working with each of you in the weeks and months ahead to build on our successes over the past ten years as we continue to meet our solemn responsibility to the American people. Thank you again for the opportunity to appear before the Committee today.