Testimony of

Deputy Secretary Jane Holl Lute

U.S. Department of Homeland Security

Before the

United States Senate

Committee on Homeland Security and Governmental Affairs

September 7, 2011

Introduction

Chairman Lieberman, Senator Collins, and distinguished Members of the Committee: thank you for the opportunity to appear before you on behalf of the Department of Homeland Security (DHS) to discuss the progress we have made in keeping our Nation safe.

I would also like to thank our many partners in the effort to ensure the safety of our Nation. DHS plays a central role in that effort, but we rely on strong partnerships throughout all levels of government, law enforcement, private industry, and with the public. We view homeland security as a whole of community enterprise, and we are fortunate to have strong partners that help us to meet our mission.

Congress is one of those essential partners. Members of Congress, and particularly this Committee, have played an extraordinary role in creating and equipping DHS and other institutions with both the authorities and the resources necessary to secure our country. You have carried forward the bipartisan spirit that marked the days after 9/11, and have provided DHS with the necessary tools, guidance, and oversight. You have always held us accountable.

Speaking of accountability, we are also thankful for the hard work of our partners at the U.S. Government Accountability Office (GAO). Along with DHS's Office of the Inspector General, GAO's audits help inform us as we mature and grow as an organization. Indeed, overwhelmingly, we tend to agree with GAO recommendations. For example, in the area of management, as a result of our auditors work and our discussions with them, we have put systems in place to ensure that DHS fulfills our missions and that our management lines of business are working.

On this important anniversary, however, we are grateful for the commitment of American citizens, who continue to be our greatest asset in the effort to keep our Nation safe. Since 9/11, countless Americans have stepped up, whether in our military, in our federal agencies including our Department of Homeland Security, and in our states, cities and communities, as first responders, law enforcement officials, and engaged citizens.

Americans know that everyone has a role to play. A commitment to American values is exemplified by the constant refrain that sums up the American call to service: "Send Me." Our challenges are shared challenges, and our successes are shared successes. Our shared goal in securing the homeland was to create a more resilient America, and we have succeeded.

Indeed, the work that has taken place at DHS and around the country since the creation of DHS in 2003 has been remarkable. Former DHS Secretaries Tom Ridge and Michael Chertoff have said that we are now in "Phase III" of this endeavor. While this hearing, and the GAO report, focuses on the successes and challenges of DHS, we actually see this as part of a broader story about the homeland security of the United States.

DHS Creation and Progress

This hearing comes at a moment of great reflection for our country as we approach the 10th anniversary of the attacks of September 11, 2001.

Following 9/11, the federal government moved quickly to develop a security framework to protect our country from large-scale attacks directed from abroad, while enhancing federal, state, and local capabilities to prepare for, respond to, and recover from threats and disasters at home.

As this Committee knows, a key element of this framework included the creation of DHS, bringing together 22 separate agencies and offices into a single, Cabinet-level Department in March 2003.

Created with the founding principle of protecting the American people from terrorist and other threats, DHS and its many partners have strengthened the homeland security enterprise to better address and defend against dynamic threats.

At DHS, five of our six primary missions align with the goals of the homeland security enterprise:

- Preventing Terrorism and Enhancing Security;
- Securing and Managing our Borders;
- Enforcing and Administering our Immigration Laws;
- Safeguarding and Securing Cyberspace; and
- Ensuring Resilience to Disasters.

Our sixth primary mission captures the operations we perform outside the homeland security enterprise to effectively execute the Department's responsibilities within other federal enterprise missions. In addition to these missions, we have focused on maturing the homeland security enterprise itself. Maturing and strengthening the homeland security enterprise includes enhancing shared awareness of risks and threats, building capable communities, fostering unity of effort, and facilitating innovative approaches and solutions through leading-edge science and technology, while ensuring the efforts aimed at securing the homeland do not diminish privacy, civil rights, or civil liberties.

In each mission area, we have made substantial progress over the past several years, adding new capabilities where none existed before 9/11, fostering greater integration and refinement and coordination of our responsibilities, and broadening the homeland security enterprise to include not just federal departments and entities, but the whole of government as well as our many non-governmental partners.

The results are clear. As a result of the many changes Congress made after 9/11, including the creation of DHS, the restructuring of our Nation's Intelligence Community, and the strengthening of the Federal Emergency Management Agency (FEMA), as well as the contributions and sacrifices of the American people, we are stronger and more resilient today.

We are a more capable Nation, and a stronger Nation. We are able to detect threats sooner, with better information, and make adjustments more quickly based on continuously updated intelligence. Today we know more about the people seeking to enter our country, the level of risk they pose, and what is needed to prevent potential threats from reaching our shores.

Our borders are stronger, enhanced by more personnel, technology, and infrastructure, as well as stronger partnerships with states and cities, border communities, and our international partners to the North and South.

Our immigration laws, while in need of reform, are being enforced according to common sense priorities we have set, which are to identify and remove criminals and those who are a threat to the American people.

We have also created a framework for securing our cyber systems and networks, and our critical infrastructure, where none previously existed. As part of this effort, we have enhanced our ability to protect federal government networks through better detection, reporting, and threat mitigation. We have engaged cyber-users at all levels, public and private, in our shared protection. And we have broadened our partnership with the private sector to protect our critical infrastructure, and established a new regulatory framework to protect high-risk chemical facilities.

We have built a more ready and resilient Nation that is able to confront major disasters in our states, cities, and communities. We have helped frontline responders become more equipped, better trained, and more unified under a new National Response Framework and Incident Command System. We have improved emergency communications. And we have provided billions of dollars in grants to support our Nation's first responders.

We have continued to integrate DHS, advancing the work that began more than eight years ago to refashion our homeland security enterprise and engage a full set of partners in the protection of our Nation.

Finally, we have represented in our programs and activities 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 it is these values that also provide a bulwark against those who threaten our safety and security.

Nevertheless, we know that we must continue to improve. As the threat against us continues to evolve, so do we. Today, then, is an opportunity to talk about some of our progress, which the GAO notes in its report, and also address some of the areas where there is more work to be done.

Preventing Terrorism and Enhancing Security

Our country has made significant progress in securing the Nation from terrorism since the September 11, 2001 attacks. This work has included constant enhancements and evolutions to our layered approach to security through the development of formalized terrorism risk

assessments, deployment of new technology, expanded data analysis capabilities, and applying intelligence to our security measures in near real time.

To understand the landscape of potential chemical, biological, radiological or nuclear (CBRN), terrorist threats, the DHS Science and Technology (S&T) Directorate has developed a first-of-its kind capability to provide DHS components as well as external federal partners with a systematic, science-based, formal assessment of CBRN terrorism risk to the Homeland.

Prior to 9/11, screening of passengers coming to the United States was limited to the Department of State visa process and the inspection of a person by an immigration officer at the port of entry. Provision of advance passenger information by airlines was voluntary and often inconsistent.

Over the past ten years, we have significantly adapted and enhanced our ability to detect threats, building a layered, risk-based system that includes a full range of identification verification measures – from visa application checks and biometric identification to the receipt of advanced passenger information and the full implementation of Secure Flight, a program that enables DHS to prescreen 100 percent of passengers on flights flying to, from, or within the United States against government watch lists.

With support from international partners and the aviation industry, we have implemented pre-departure programs for U.S. bound flights as well as enhanced security measures to strengthen the safety and security of all passengers.

These new measures, which cover 100 percent of passengers traveling by air to the United States, utilize continuously updated, threat-based intelligence along with multiple layers of security, both seen and unseen, to more effectively mitigate evolving terrorist threats.

Prior to 9/11, there also was no advance screening of passengers seeking admission under the Visa Waiver Program (VWP), which enables nationals of 36 designated countries to travel to the United States for stays of 90 days or less without obtaining a visa. In 2008, DHS implemented the Electronic System for Travel Authorization (ESTA) to screen prospective VWP travelers against several databases, including the terrorist watchlist; lost and stolen passports; visa revocations; previous VWP refusals; and public health records.

In addition, prior to 9/11, limited federal security requirements existed for cargo or baggage screening. Today, all checked and carry-on baggage aboard aircraft is screened for explosives. Increased levels of frontline security personnel at the passenger checkpoints and new technologies have significantly enhanced security as well. Today, TSA personnel serve on the frontlines at over 450 U.S. airports.

We also have taken significant action to counter the threat of nuclear, biological, and radiological weapons or materials entering the United States. When the Department was formed, we scanned only 68 percent of arriving trucks and passenger vehicles along the Northern border for radiological and nuclear threats. No scanning systems were deployed to the Southwest border and only one was deployed to a seaport. Today, these systems scan 100 percent of all

containerized cargo and personal vehicles arriving in the U.S. through land border ports of entry, as well as over 99 percent of arriving sea containers.

Since the anthrax attacks 10 years ago, we also have made great strides in protecting the Nation from, and preparing federal, state, and local governments to respond to biological attacks. In 2003, the Department stood up the BioWatch system—a federally-managed, locally-operated, nationwide environmental surveillance system designed to detect the intentional release of aerosolized biological agents which is currently operational in approximately 30 cities and states.

The terrorist threats facing the United States have evolved significantly over the last decade, and continue to evolve. In addition to the direct threats from al-Qa‘ida, foreign terrorist groups affiliated with al-Qa‘ida, as well as individual violent extremist thought leaders, are seeking to recruit or inspire individuals in the Homeland to carry out attacks with little or no warning.

The threat posed by violent extremism is neither constrained by international borders nor limited to any single ideology. Groups and individuals inspired by a range of religious, political, or other ideological beliefs have promoted and used violence against the Homeland. Increasingly sophisticated use of the Internet, mainstream and social media, and information technology by violent extremists adds an additional layer of complexity.

To counter violent extremism (CVE), DHS is working with a broad range of partners to gain a better understanding of the behaviors, tactics, and other indicators that could point to potential terrorist activity within the United States, and the best ways to mitigate or prevent that activity. Our approach to CVE emphasizes the strength of local communities.

We begin with the premise that well-informed and -equipped families, communities, and local institutions represent the best defense against terrorist ideologies. And while our primary purpose is to prevent a terrorist and violent extremist attack by an individual or group recruited by a violent extremist organization, or inspired by an extremist ideology, we also support strong and resilient communities as important ends themselves.

To implement this approach, we are working closely with our federal and international partners, as well as our many partners at the community, state, local, and tribal levels across the country. We are an important partner in supporting the National Strategy on Empowering Local Partners to Prevent Violent Extremism, which President Obama released on August 3, 2011.

Securing and Managing our Borders

Protecting our Nation’s borders—land, air, and sea—from the illegal entry of people, weapons, drugs, and contraband is vital to homeland security, as well as economic prosperity.

To meet this responsibility, we have deployed unprecedented levels of personnel, technology, and resources to the Southwest border. At the same time, we have made critical security improvements along the Northern border, investing in additional Border Patrol agents, technology, and infrastructure while also strengthening efforts to increase the security of the Nation’s maritime borders.

Today, the Border Patrol has more staff than at any time in its 87-year history. Along the Southwest border, DHS has increased the number of civilian boots on the ground from approximately 9,100 Border Patrol agents in 2001 to more than 17,700 today.

Under the Southwest Border Initiative, we have doubled the number of personnel assigned to Border Enforcement Security Task Forces (BESTs), which leverage federal, state, local, tribal and foreign law enforcement and intelligence resources in an effort to identify, disrupt, and dismantle transnational criminal organizations that seek to exploit vulnerabilities along the U.S. borders and threaten the overall safety and security of the American public.

We have increased the number of U.S. Immigration and Customs Enforcement (ICE) intelligence analysts along the border focused on cartel violence; quintupled deployments of Border Liaison Officers to work with their Mexican counterparts; begun screening 100 percent of southbound rail shipments for illegal weapons, drugs, and cash; and expanded Unmanned Aircraft System (UAS) coverage to the entire Southwest border. There were no deployments of UASs along the Southwest border prior to 9/11.

Further, the $600 million supplemental funding requested by the Administration and passed by Congress in 2010, with nearly $400 million targeted for DHS, is enabling us to continue to add technology, personnel, and infrastructure to the Southwest border. These resources include 1,000 additional Border Patrol Agents; 250 new U.S. Customs and Border Protection officers at U.S. ports of entry; 250 new ICE agents focused on transnational crime; improved tactical communications systems; two new forward operating bases to improve coordination of border security activities; and additional CBP UASs.

While this work is not yet complete, every key metric currently available shows that these border security efforts are producing significant results. Illegal immigration attempts, as measured by Border Patrol apprehensions, have decreased 36 percent in the past two years, and are less than one third of what they were at their peak. Seizures of drugs, weapons and currency have increased across the board. The S&T Directorate continues to improve current detection technologies and look at advanced sensors and systems for CBP and Coast Guard in order to provide a more effective and cost efficient means for securing our land and maritime borders.

In July 2011, the Obama Administration also released its most recent National Southwest Border Counternarcotics Strategy, which provides the Administration's overarching framework to address the threats posed by the illicit narcotics trade. And DHS has forged historic agreements with the Department of Justice (DOJ), increasing coordination between ICE and the Bureau of Alcohol, Tobacco, Firearms and Explosives and the Drug Enforcement Administration (DEA) on important Southwest border issues such as combating arms trafficking, bolstering information sharing and providing ICE agents the authority to work on important drug trafficking cases.

In addition, we have signed numerous bilateral agreements and declarations to bolster and deepen collaboration with Mexico in the areas of enforcement, planning, information and intelligence sharing, joint operations, and trade facilitation along the Southwest border.

On our Northern border, we continue to invest in personnel, technology, and infrastructure, and to strengthen cooperation with federal, state/provincial, tribal, and private sector partners on both sides of the border. These achievements have resulted in a more secure Northern border that facilitates legitimate travel and trade.

Currently, CBP has more than 2,200 Border Patrol agents on the Northern border, a 500 percent increase since 9/11. CBP also has nearly 3,700 CBP officers managing the flow of people and goods across ports of entry and crossings along the Northern border.

The Department has also continued to deploy technology along the Northern border, including thermal camera systems, Mobile Surveillance Systems, Remote Video Surveillance Systems, and long-range CBP Predator-B unmanned aircraft patrols. In February 2011, President Obama and Canadian Prime Minister Harper announced a landmark "Shared Vision for Perimeter Security and Economic Competitiveness" that sets forth how the two countries will manage shared homeland and economic security in the 21st century. This shared vision, or "Beyond the Border," continues to protect individual privacy and civil liberties while securing the flows of trade and travel that strengthens North American perimeter security and the overall economy.

The U.S. Coast Guard continues to work with other federal, state, local and tribal partners to enhance security along the U.S. maritime border and uses interagency partnerships and international bilateral agreements to accomplish this mission. The Coast Guard leverages its unique maritime security authorities, capabilities and partnerships to mitigate risk and improve security in our domestic ports, on the high seas, and in ports abroad through a layered security approach. Closer to shore, the Coast Guard patrols our ports, conducts vessel escorts, and inspects vessels and facilities.

With respect to identity document security, DHS also has taken significant steps to strengthen security, reduce fraud and improve the reliability and accuracy of personal identification documents while enhancing privacy safeguards. For example, we have fundamentally transformed the way travelers enter the United States from within the Western Hemisphere through implementation of the Western Hemisphere Travel Initiative (WHTI) and from other countries around the world through the VWP, Visa Security Program and US-VISIT biometric identity and verification process.

Prior to the implementation of WHTI, there was no standard documentary requirement for U.S. or most Canadian citizens to enter the United States from within the Western Hemisphere; travelers could present any one of numerous documents or simply make an oral declaration of citizenship. In 2005, DHS checked five percent of all passengers crossing land borders by vehicles against law enforcement databases. Today, due to WHTI, the national query rate is over 97 percent.

Enforcing and Administering our Immigration Laws

What we do to protect our borders is inseparable from immigration enforcement in the interior of our country, and both are critical to an effective immigration system.

Our approach to immigration enforcement has focused on identifying criminal aliens and those who pose the greatest risk to our communities, and prioritizing them for removal. In addition, we have worked to ensure that employers have the tools they need to maintain a legal workforce, and face penalties if they knowingly and repeatedly violate the law. And we have made significant changes to our immigration detention system, to recognize the basic differences between immigration violators – from non-violent aliens to hardened, violent criminals and gang members – and house them accordingly in order to optimize the safety and security of other detainees and the facilities' staff.

Like our actions at the border, our interior enforcement efforts are achieving major results. In Fiscal Years 2009 and 2010, ICE removed more illegal immigrants from our country than ever before, with more than 779,000 removals nationwide in the last two years. Most importantly, more than half of those aliens removed last year – upwards of 195,000 – were convicted criminals, the most ever removed from our country in a single year.

We also have stepped up our efforts to target employers who repeatedly and egregiously break the law, last year arresting a record number of employers who knowingly hire illegal aliens. ICE has significantly expanded its use of I-9 audits, which are used to investigate employers suspected of employing illegal aliens. Since January 2009, ICE has audited more than 3,600 employers suspected of employing unauthorized aliens, debarred more than 260 companies and individuals, and imposed approximately $56 million in financial sanctions – more than the total amount of audits and debarments than during the entire previous administration.

We also have strengthened the efficiency and accuracy of E-Verify – our on-line employment verification system managed by U.S. Citizenship and Immigration Services (USCIS). More than 249,000 employers are enrolled in E-Verify, representing more than 857,000 locations. More than 1,300 new employers enroll each week and the number of employers enrolled in E-Verify has more than doubled each fiscal year since 2007.

To combat the growing problem of smuggling and trafficking, we also have continued to conduct targeted enforcement operations while launching national public awareness campaigns, including in Central and South America, to shine a spotlight on this unconscionable crime. DHS also launched the Blue Campaign to Combat Human Trafficking, a national initiative focused on protection, prevention, and prosecution.

Of course, our country is a nation of immigrants, and we must remain open and welcoming to new immigrants while supporting their integration into our society. USCIS has taken a number of actions to improve its ability to meet these goals. By streamlining and modernizing operations, USCIS is now processing applications for naturalization and other critical immigration benefits more rapidly, meeting or exceeding performance goals. As a customer-focused agency, USCIS also has taken steps to improve one of its primary interfaces with the public through its website: www.uscis.gov.

USCIS also has made security enhancements to some of its key identity documents to prevent counterfeiting, obstruct tampering, and facilitate quick and accurate authentication. And USCIS continues to enhance fraud detection and national security capabilities to ensure that immigration

benefits are not granted to individuals who pose a threat to national security. For example, USCIS has embedded Fraud Detection and National Security officers in nine other government agencies to increase information sharing and collaboration efforts that enhance law enforcement and intelligence operations.

Finally, USCIS has continued to naturalize thousands of new Americans each year, including record numbers of members of our Nation's Armed Forces. In FY 2010, USCIS granted citizenship to 11,146 members of the U.S. Armed Forces at ceremonies in the United States and 22 countries abroad. This figure represents the highest number of service members naturalized in any year since 1955.

These improvements to our legal immigration system, coupled with our efforts to secure the border and enforce immigration laws in the interior, are producing significant results. We know that more is required to fully address our Nation's immigration challenges. Ultimately, Congress needs to take up reforms to our immigration system to address long-standing, systemic problems with our Nation's immigration laws.

Safeguarding and Securing Cyberspace

Today's threats to cybersecurity require the engagement of our entire society—from government and law enforcement to the private sector and importantly, members of the public— to block malicious actors while bolstering defensive capabilities.

DHS is responsible for protecting the federal executive branch civilian agencies, and assisting in the protection of the Nation's critical infrastructure and critical information systems where the government maintains sensitive information and which provide services to the American people and support the financial services, energy, and defense industries.

Over the past ten years, DHS has made significant strides in enhancing the security of the Nation's critical physical infrastructure as well as its cyber infrastructure and networks. In October 2010, DHS and the Department of Defense (DOD) signed a Memorandum of Agreement to align and enhance America's capabilities to protect against threats to critical civilian and military computer systems and networks. The Agreement embeds DOD cyber analysts within DHS and sends DHS privacy, civil liberties, and legal personnel to DOD's National Security Agency to strengthen the Nation's cybersecurity posture and ensure the protection of fundamental rights.

In partnership with the private sector, the U.S. Computer Emergency Readiness Team (US-CERT) continues to take proactive measures to stop possible threats by developing and sharing standardized threat indication, prevention, mitigation, and response information products with its governmental and private sector partners.

DHS also has developed the first-ever National Cyber Incident Response Plan in September 2010 to coordinate the response of multiple federal agencies, state and local governments, and hundreds of private firms, to incidents at all levels.

In October 2009, DHS also opened the new National Cybersecurity and Communications Integration Center (NCCIC) —a 24-hour, DHS-led coordinated watch and warning center to serve as the Nation's principal hub for organizing cyber response efforts and maintaining the national cyber and communications common operational picture.

DHS also utilizes the National Cybersecurity Protection System, of which the EINSTEIN intrusion detection system is a key component, to protect the dot-gov domains. When fully deployed, the latest version of the EINSTEIN system, the first version of which was deployed in 2004, will help block malicious actors from accessing federal executive branch civilian agencies. At the same time, DHS is working closely with those agencies to bolster their defensive capabilities.

Additionally, as part of the Comprehensive National Cybersecurity Initiative, DHS is working to reduce and consolidate the number of external connections that federal agencies have to the Internet through the Trusted Internet Connection (TIC) initiative. And to meet our future workforce needs, DHS is also building a world-class cybersecurity team by hiring a diverse group of cybersecurity professionals—computer engineers, scientists, and analysts—to secure the nation's digital assets and protect against cyber threats to Critical Infrastructure and Key Resources (CIKR).

Finally, DHS is committed to increasing public awareness about cybersecurity and empowering individuals and enterprises across cyber networks to enhance their own security operations. In 2010, the Department launched the *"Stop. Think. Connect."* public cybersecurity awareness campaign to increase public understanding of cyber threats and promote simple steps the public can take to increase their safety and security online. Additionally, DHS S&T co-sponsors national and regional cybersecurity competitions at the high school and collegiate levels, to educate young individuals who can design secure systems and create sophisticated tools needed to prevent malicious acts.

Ensuring Resilience To Disasters

DHS provides the coordinated, comprehensive Federal response in the event of a terrorist attack, natural disaster or other large-scale emergency while working with Federal, state, local, and private sector partners to ensure a swift and effective recovery effort. Over the past ten years, we have worked to strengthen our Nation's ability to prepare for, protect against, respond to, recover from and mitigate major emergencies and disasters of all kinds, at all levels.

To strengthen emergency preparedness and response planning, we issued the National Response Framework in January 2008, which builds on predecessor plans that did not exist prior to 9/11. We also revised the National Incident Management System in December 2008.

We have substantially strengthened FEMA, giving it – with the help and guidance of this Committee – a more effective structure, better tools and technology, new logistics capabilities, more effective sheltering planning, and a "forward leaning" posture that pushes more assets and resources into the field in advance of a disaster when capabilities of the States are overwhelmed.

To support state, local, and tribal governments and the private sector in strengthening preparedness for acts of terrorism, major disasters, and other emergencies, we have awarded more than $31 billion in preparedness grant funding since 2003. This funding is based on risk to build and sustain targeted capabilities to prevent, protect against, respond to, and recover from threats or acts of terrorism.

In addition, to enhance emergency and interoperable communications, we developed the National Emergency Communications Plan in coordination with more than 150 public safety practitioners at all levels and across responder disciplines. The National Emergency Communications Plan is our Nation's first nationwide strategic plan to improve emergency communications and drive progress at all levels of government. We have also made over $4 billion in grants for interoperable communications available and increasingly aligned them with national and state plans.

DHS Transformation and Integration

Finally, we have taken significant steps to create a unified and integrated Department, focusing on accountability, transparency and leadership development to enhance our mission performance. We are implementing a comprehensive, strategic management approach to enhance the people, structures, and processes needed to meet our mission. This approach integrates and aligns our business functions at the Departmental and Component levels and is focused on three key elements:

1. Acquisition Enhancement: Improving upon the current Department process and procedures – particularly the "front end" requirements and the "back end" program management to minimize risk, encourage fiscal responsibility, and execution across the acquisition life-cycle.

2. Financial Enhancement: Improving our financial systems and capabilities in both the management directorate and the components.

3. Human Capital Management Enhancement: Making sure we have the right people in the right positions at the right time, with the proper workforce balance between DHS and contract employees.

DHS has a strong commitment to effective acquisition management. In August, 2007, we established the Acquisition Program Management Division to help strengthen acquisition management within DHS. In the future we will establish an Investment Review Board to oversee the status of all acquisition investments. We also have revised our acquisition management oversight policies to include more detailed guidance to inform our acquisition decisions.

We are also firmly committed to strengthening Department-wide financial management, and we have made progress in this area. The results of our FY 2010 financial annual audit have demonstrated steady progress toward sound financial results.

For example, we have reduced the number of material weakness conditions over financial reporting by half since FY 2005. We also have formalized Department-wide uniform processes and procedures to strengthen accounting and financial reporting.

To meet human capital needs, we issued our Workforce Strategy for Fiscal Years 2011-2016 in December 2010, which contains the Department's workforce goals, objectives, and performance measures for human capital management. We are also developing component operational plans and tracking those plans against a common set of performance measures. In addition, we have developed a diversity council, among other initiatives, to ensure we have a workforce that reflects the diversity of America.

Conclusion

The guiding philosophy behind the homeland security enterprise – shared responsibility – means that we share both responsibility and success among our many partners in the homeland security effort.

The complexity of this challenge, and its import, not only to the United States but to nations that look to us for guidance, makes it essential that we succeed. It is only through a whole of community approach that we can build the necessary capabilities, countermeasures, and sustained public and private sector engagement required to keep our country safe in the face of evolving threats, and to build the resilience needed to bounce back from threats, challenges, and setbacks.

This Committee has been instrumental to our ability to achieve our mission thus far, and your partnership and support will be essential in the future. We look forward to continuing our work with you, and we remain grateful for all that you have done to help us succeed over the past eight years and since 9/11.