IMPLEMENTING 9/11 COMMISSION RECOMMENDATIONS

Progress Report 2011

Release Date: July 21, 2012

Highlights of Our Progress

Learn more about the progress we've made in our mission areas:

Preventing Terrorism and Enhancing Security

Read the Implementing 9/11 Commission Recommendations, Progress Report 2011

The Department of Homeland Security (DHS) and its many partners across the federal government, public and private sectors, and communities across the country and around the world have worked since 9/11 to build a new homeland security enterprise to better mitigate and defend against dynamic threats, minimize risks, and maximize the ability to respond and recover from attacks and disasters of all kinds.

Together, these efforts have provided a strong foundation to protect communities from terrorism and other threats, while safeguarding the fundamental rights of all Americans.

While threats persist, our nation is stronger than it was on 9/11, more prepared to confront evolving threats, and more resilient in the face of our continued challenges.

Progress Made Since 9/11

Protecting the United States from terrorism is the founding mission of the Department of Homeland Security. While America is stronger and more resilient as a result of a strengthened homeland security enterprise, 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 home-made bomb or as sophisticated as a biological threat or coordinated cyber attack. More and more, state, local, and tribal law enforcement officers, as well as citizens, businesses, and communities are on the front lines of detection and prevention. Protecting the nation is a shared responsibility and everyone can contribute by staying informed and aware of the threats the country faces. Homeland security starts with hometown security—and we all have a role to play.

Building the Homeland Security Enterprise

- **Fusion Centers**: DHS supports state and major urban area fusion centers through personnel, training, technical assistance, exercise support, security clearances, connectivity to federal systems, technology, and grant funding.
- **Nationwide Suspicious Activity Reporting Initiative**: An administration effort to train state and local law enforcement to recognize behaviors and indicators related to terrorism, crime and other threats; standardize how those observations are documented and analyzed; and enhance the sharing of those reports with law enforcement across the country.
- **Grant Funding**: Since fiscal year 2003, DHS has awarded more than $31 billion in preparedness grant funding based on risk to build and sustain targeted capabilities to prevent, protect against, respond to, and recover from threats or acts of terrorism.

Preventing Terrorist Travel and Improving Passenger Screening

- **Advance Passenger Information and Passenger Name Record Data**: To identify high-risk travelers and facilitate legitimate travel, DHS requires airlines flying to the United States to provide Advance Passenger Information and Passenger Name Record (PNR) Data prior to departure. During 2008 and 2009, PNR helped the United States identify individuals with potential ties to terrorism in more than 3,000 cases, and in fiscal year 2010, approximately one quarter of those individuals denied entry to the United States for having ties to terrorism were initially identified through the analysis of PNR.

- **Visa Security Program**: Through the Visa Security Program (VSP), with concurrence from the Department of State, ICE deploys trained special agents overseas to high-risk visa activity posts in order to identify potential terrorist and criminal threats before they reach the United States. The VSP is currently deployed to 19 posts in 15 countries.

- **Pre-Departure Vetting:** DHS has strengthened its in-bound targeting operations to identify high-risk travelers who are likely to be inadmissible to the United States and to recommend to commercial carriers that those individuals not be permitted to board a commercial aircraft through its Pre-Departure program. Since 2010, CBP has identified over 2,800 passengers who would likely have been found inadmissible upon arrival to the United States.

- **Secure Flight**: Fulfilling a key 9/11 Commission recommendation, DHS fully implemented Secure Flight in 2010, in which TSA prescreens 100 percent of passengers on flights flying to, from, or within the United States against government watchlists before travelers receive their boarding passes. Prior to Secure Flight, airlines were responsible for checking passengers against watchlists. Through Secure Flight, TSA now vets over 14 million passengers weekly.

- **Enhanced Explosives Screening:** Prior to 9/11, limited federal security requirements existed for cargo or baggage screening. Today, TSA screens 100 percent of all checked and carry-on baggage for explosives. Through the Recovery Act and annual appropriations, TSA has accelerated the deployment of new technologies to detect the next generation of threats, including Advanced Imaging Technology units, Explosive Detection Systems, Explosives Trace Detection units, Advanced Technology X-Ray systems, and Bottled Liquid Scanners.

Strengthening Surface Transportation Security

- **Visible Intermodal Prevention and Response Teams**: TSA has 25 multi-modal Visible Intermodal Prevention and Response (VIPR) Teams working in transportation sectors across the country to prevent or disrupt potential terrorist planning activities. Since the VIPR program was created in 2008, there have been over 17,700 operations performed.

- **Baseline Surface Transportation Security Assessments**: Since 2006, TSA has completed more than 190 Baseline Assessments for Security Enhancement for transit, which provides a comprehensive assessment of security programs in critical transit systems.

Strengthening Global Supply Chain Security

- **Air Cargo Screening**: Fulfilling a requirement of the 9/11 Act, 100 percent of all cargo transported on passenger aircraft that depart U.S. airports is now screened commensurate with screening of passenger checked baggage and 100 percent of high risk cargo on international flights bound for the United States is screened.

- **Container Security Initiative**: The Container Security Initiative (CSI), currently operational in 58 foreign seaports in 32 countries, identifies and screens U.S.-bound maritime containers that pose a potential risk.

Detecting and Preventing Biological, Radiological, and Nuclear Threats

- **Detection at Ports of Entry:** DHS has deployed radiation detection technologies to seaports, land border ports, and mail facilities around the world. These systems scan 100 percent of all containerized cargo and personal vehicles arriving in the U.S. through land ports of entry, as well as over 99 percent of arriving sea containers.

- **State and Local Radiological Emergency Preparedness:** DHS's Domestic Nuclear Detection Office has made radiological and nuclear detection training available to over 15,000 state and local officers and first responders.

- **BioWatch**: The Department's BioWatch system is a federally-managed, locally-operated, nationwide bio-surveillance system designed to detect the intentional release of aerosolized biological agents.

Protecting Critical Infrastructure

- **Chemical Facility Anti-Terrorism Standards**: DHS has implemented Chemical Facility Anti-Terrorism Standards to regulate security at high-risk chemical facilities. To date, approximately 4,500 facilities have been preliminarily identified as high-risk, resulting in the development and submission of Security Vulnerability Assessments.

- **Critical Infrastructure Security Assessments**: DHS has conducted more than 1,900 security surveys and 2,500 vulnerability assessments of the nation's critical infrastructure to identify potential vulnerabilities and provide recommendations on protective measures.

- **Training and Education**: DHS has developed a variety of infrastructure protection training and educational tools for its partners at the state and local level. In total, more than 35,000 partners have taken risk mitigation training on a range of topics.

Strengthening the Homeland Security Enterprise

Read the Implementing 9/11 Commission Recommendations, Progress Report 2011

The Department of Homeland Security (DHS) and its many partners across the federal government, public and private sectors, and communities across the country and around the world have worked since 9/11 to build a new homeland security enterprise to better mitigate and defend against dynamic threats, minimize risks, and maximize the ability to respond and recover from attacks and disasters of all kinds.

Together, these efforts have provided a strong foundation to protect communities from terrorism and other threats, while safeguarding the fundamental rights of all Americans.

While threats persist, our nation is stronger than it was on 9/11, more prepared to confront evolving threats, and more resilient in the face of our continued challenges.

Progress Made Since 9/11

Over the past several years, DHS and our partners have evolved and strengthened our homeland security enterprise in order to better defend against evolving terrorist threats. This enterprise extends far beyond DHS and the many departments and agencies that contribute to our homeland security mission. A key part includes working directly with law enforcement, state and local leaders, community-based organizations, private sector and international partners.

Federal Government Partnerships

Within the federal government, many departments and agencies contribute to the homeland security mission. The nation's armed forces are on the front lines of homeland security by degrading al-Qa'ida's capabilities to attack the United States and targets throughout the world. 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 Administration has made critical enhancements to the federal watchlisting systems and to the coordination of the Federal government's counterterrorism efforts. The Federal homeland security enterprise also includes the strong presence of the Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI), whose role in leading terrorism investigations has led to the arrest of more than two-dozen Americans on terrorism-related charges since 2009.

State, Local, Tribal, and Territorial Partners

DHS has focused on getting resources and information out of Washington, D.C. and into the hands of state and local law enforcement, to provide them with the tools to identify and combat threats in their communities. Because state and local law enforcement are often in the best position to notice the first signs of a planned attack, homeland security efforts must be integrated into the police work that they do every day, providing officers on the front lines with a clear understanding of the tactics, behaviors, and other indicators that could point to terrorist activity.

DHS supports these efforts through robust information sharing with public and private sector partners; fusion centers to build analytical capability at the state and local level; participation in the Nationwide Suspicious Activity Reporting Initiative – an Administration effort to train state and local law enforcement to recognize behaviors and indicators related to terrorism, crime and other threats, and FBI-led Joint Terrorism Task Forces (JTTF) that investigate terrorist threats. DHS also helps state and local partners build and sustain capabilities to prevent, protect against, respond to, and recover from threats or acts of terrorism through grant funding, training and technical assistance. In 2009, DHS designated Tribal liaisons in every operational component to work directly with tribal communities. In 2011, DHS announced a new Tribal Consultation Policy outlining the guiding principles under which all elements of the Department will engage with sovereign tribal governments.

Private Sector Outreach

The private sector is an integral component of the homeland security enterprise, and through the Department's private sector office, DHS has improved coordination of private sector engagement across the Department, facilitating more effective and rapid communication with key organizations and bolstering regionally-focused information sharing efforts. Since 9/11, DHS also has prioritized private sector preparedness through programs such as the Voluntary Private Sector Preparedness Accreditation and Certification Program (PS-Prep™), Ready Business, the development and deployment of new technologies, and by incorporating private sector partners from the outset when developing new policies, programs and initiatives.

International Efforts

DHS works closely with international partners, including major multilateral organizations and global businesses to strengthen the security of the networks of global trade and travel upon which the nation's economy and communities rely. DHS has enhanced the security of the aviation system, not only in airports throughout the United States, but also in airports abroad, by working directly with foreign governments, international organizations, and the aviation industry to raise aviation security standards. The Administration's global supply chain initiative is building on many of these partnerships, including work with International Civil Aviation Organization (ICAO), World Customs Organization (WCO), and International Maritime Organization (IMO).

Public Engagement

The public also plays a key role in our strengthened homeland security enterprise. Through the nationwide expansion of the "If You See Something, Say Something™" campaign, which was originally implemented by New York City's Metropolitan Transportation Authority, DHS is raising public awareness of indicators of terrorism and crime while emphasizing the importance of reporting suspicious activity to the proper law enforcement authorities. Recently, DHS replaced the color-coded alert system with the new National Terrorism Advisory System (NTAS)–a robust terrorism advisory system that provides timely information to the public and the private sector, as well as to state, local and tribal governments about credible terrorist threats and recommended security measures.

Enforcing and Administering Our Immigration Laws

Read the Implementing 9/11 Commission Recommendations, Progress Report 2011

The Department of Homeland Security (DHS) and its many partners across the federal government, public and private sectors, and communities across the country and around the world have worked since 9/11 to build a new homeland security enterprise to better mitigate and defend against dynamic threats, minimize risks, and maximize the ability to respond and recover from attacks and disasters of all kinds.

Together, these efforts have provided a strong foundation to protect communities from terrorism and other threats, while safeguarding the fundamental rights of all Americans.

While threats persist, our nation is stronger than it was on 9/11, more prepared to confront evolving threats, and more resilient in the face of our continued challenges.

Progress Made Since 9/11

Through a multi-layered, risk based system, the Department of Homeland Security (DHS) has taken significant steps to prevent dangerous individuals from traveling to, entering and remaining in the United States and to ensure that immigration benefits are not granted to individuals who pose a threat to national security. The Department's efforts have focused on combating immigration fraud, improving the reliability and accuracy of personal identification documents, and enhancing information sharing while enhancing privacy safeguards.

Combating Immigration Fraud

- **Pre-Screening:** Visa applicants, those seeking to enter the U.S. at a port of entry, refugee, and asylum applicants are subject to rigorous background vetting, biographic, and biometric checks–including checks against records obtained by the Department of Defense (DOD), in Iraq and Afghanistan.

- **Permanent Resident Card**: The new Permanent Resident Card (commonly referred to as a "green card"), implemented in 2010, includes a radio frequency identification tag that allows Customs and Border Protection to quickly access the electronic records of travelers seeking to enter the United States and includes new security features that reduce the risks of counterfeiting, tampering, and fraud.

- **Employment Authorization Document**: U.S. Citizenship and Immigration Services (USCIS) updated the Employment Authorization Document by adding a machine-readable zone that will allow border control officers to more efficiently identify people who have already been approved for immigration benefits and who have been reviewed previously by USCIS officers.

- **Forensic Document Laboratory**: The Immigration and Customs Enforcement (ICE) Forensic Document Laboratory (FDL) is the federal government's forensic crime laboratory dedicated exclusively to fraudulent document detection and deterrence. USCIS works closely with the FDL to enhance its ability to identify fraudulent documents submitted in support of applications and petitions seeking immigration benefits.

- **Validation Instrument for Business Enterprises**: USCIS implemented a new tool to enhance adjudications of certain employment-based immigration petitions known as the Web-based Validation Instrument for Business Enterprises (VIBE). VIBE limits the need to request supplemental evidence directly from petitioning organizations while accelerating the adjudicative vetting process and enhancing the agency's anti-fraud capabilities.

- **International Student and Exchange Visitor Program**: ICE manages the International Student and Exchange Visitor Program (SEVP), which tracks and monitors the status and activities of nonimmigrant students and exchange visitors to ensure that only legitimate foreign students or exchange students gain entry to the United States and that they abide by the terms of their visas while here.

Strengthening Identification Verification

- **Western Hemisphere Travel Initiative**: In 2009, DHS successfully implemented the Western Hemisphere Travel Initiative (WHTI) for land and sea travel to the U.S., requiring that U.S., Mexican and Canadian citizens present a passport or other secure travel document that denotes identity and citizenship when entering the U.S. Prior to WHTI, U.S. or Canadian travelers could present any of numerous documents and 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.

Biometric Information-Sharing

- **Biometrics at Sea**: The U.S. Coast Guard (USCG) has implemented a mobile biometrics collection system to identify undocumented migrants and match them against known databases of past criminal and immigration violations as well as terrorist watchlists. Through June 2011, the USCG has identified more than 900 individuals who were enrolled in the US-VISIT database as prior felons, violators of U.S. immigration laws, or other persons of interest and referred to law enforcement authorities for appropriate action.

- **International Agreements:** DHS and the Department of State have worked with Australia, Canada, New Zealand, and the United Kingdom to develop routine sharing of biometric information collected for immigration purposes. To date, this effort has identified many cases of routine immigration fraud, as well as dangerous people traveling under false identities.

Securing and Managing Our Borders

Read the Implementing 9/11 Commission Recommendations, Progress Report 2011

The Department of Homeland Security (DHS) and its many partners across the federal government, public and private sectors, and communities across the country and around the world have worked since 9/11 to build a new homeland security enterprise to better mitigate and defend against dynamic threats, minimize risks, and maximize the ability to respond and recover from attacks and disasters of all kinds.

Together, these efforts have provided a strong foundation to protect communities from terrorism and other threats, while safeguarding the fundamental rights of all Americans.

While threats persist, our nation is stronger than it was on 9/11, more prepared to confront evolving threats, and more resilient in the face of our continued challenges.

Progress Made Since 9/11

Protecting the nation's borders—land, air, and sea—from the illegal entry of people, weapons, drugs, and contraband is vital to our homeland security, as well as economic prosperity. Over the past several years, DHS has deployed unprecedented levels of personnel, technology, and resources to the Southwest border. At the same time, DHS has 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.

Southwest Border

Investing in Personnel, Technology, and Infrastructure

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

- Immigration and Customs Enforcement (ICE) has deployed a quarter of all its personnel to the Southwest border region – the most ever- doubling the number of personnel assigned to Border Enforcement Security Task Forces which work to dismantle criminal organizations along the border; increasing the number of intelligence analysts focused on cartel violence; and quintupling deployments of Border Liaison Officers to work with their Mexican counterparts.

- Customs and Border Protection (CBP) has deployed dual detection canine teams, which identify firearms and currency, 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.

- CBP now screens 100 percent of southbound rail shipments for illegal weapons, drugs, and cash, has expanded Unmanned Aircraft System (UAS) coverage to the entire Southwest border and completed 650 miles of fencing.

- President Obama authorized the temporary deployment of up to 1,200 additional National Guard personnel as a bridge to longer-term enhancements in border protection, and law enforcement personnel from DHS to target illicit networks' trafficking in people, drugs, illegal weapons, money, and the violence associated with these illegal activities.

Fewer Apprehensions and Increased Interdiction of Drugs, Weapons, and Currency

- 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.

- Over the past two and a half years, DHS has seized 75 percent more currency, 31 percent more drugs, and 64 percent more weapons along the Southwest border as compared to the last two and a half years during the previous Administration.

International Partnerships

- In 2010, Presidents Obama and Calderon issued a Declaration on 21st Century Border Management, to pursue initiatives that will expedite the legitimate flow of people and goods and focus law enforcement resources on those people and goods that represent the highest risk or about which officials know the least.

- Secretary Napolitano and her Mexican counterparts have signed numerous bilateral agreements and declarations to deepen cooperation and collaboration in the areas of enforcement, planning, information and intelligence sharing, joint operations, and trade facilitation along the Southwest border.

Northern Border

- **International Partnerships:** In February 2011, President Obama and Prime Minister Harper of Canada signed the "Shared Vision for Perimeter Security and Economic Competitiveness." The "Shared Vision" emphasizes shared responsibility for the safety, security, and resilience of the United States and Canada by addressing threats at the earliest point possible; facilitating trade, economic growth, and jobs; collaborating on integrated cross-border law enforcement; and partnering to secure and strengthen the resilience of critical infrastructure and cybersecurity.

- **Boots on the Ground:** Currently, CBP has more than 2,200 Border Patrol agents on the Northern border, a 500 percent increase since 9/11. In addition, there are nearly 3,700 CBP Officers

managing the flow of people and goods across ports of entry and crossings along the Northern border.

- **Ports of Entry:** CBP is using Recovery Act funds to modernize more than 35 land ports of entry along the Northern border to meet current security and operational needs.

- **Technology:** DHS has deployed thermal camera systems, Mobile Surveillance Systems, and Remote Video Surveillance Systems along the Northern border.

- **Aerial Coverage:** Approximately 950 miles along the Northern border from Washington to Minnesota are currently covered by unmanned aircraft, in addition to approximately 200 miles along the northern border in New York and Lake Ontario—none of which were covered prior to the creation of DHS.

Maritime Security

- The United States Coast Guard (USCG) secures our nation's maritime borders through a layered security system that begins beyond the country's physical borders. At-sea presence deters potential threats, provides mobile surveillance coverage, increases warning time, engages smugglers at the earliest point possible, and enables USCG to address potential threats before they can cause harm to the United States.

- USCG's Maritime Security and Response Operations include waterborne and aerial patrols as well as armed escorts of hazardous cargos and passenger vessels in order to reduce the risk of terrorism to the U.S. Marine Transportation System, critical infrastructure and key resources.

- USCG has increased the presence and capabilities of maritime forces to address threats through the establishment of the Deployable Operations Group, which can respond rapidly to terrorist and weapons of mass destruction threats as well as Maritime Safety and Security Teams at critical U.S. ports, which focus on domestic maritime threats and post-incident response.

Border Security

- **Western Hemisphere Travel Initiative WHTI:** In 2009, DHS successfully implemented the Western Hemisphere Travel Initiative (WHTI) for land and sea travel to the U.S., requiring that U.S., Mexican and Canadian citizens present a passport or other secure travel document that denotes identity and citizenship when entering the U.S. Prior to WHTI, U.S. or Canadian travelers could present any of numerous documents and simply make an oral declaration of citizenship.

- **Radiation Detection:** Customs and Border Protection has deployed Radiation Portal Monitors and other radiation detection technologies to seaports, land border ports, and mail facilities around the world. In 2003, these systems scanned only 68 percent of arriving trucks and passenger vehicles along the Northern border, no 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 ports of entry, as well as over 99 percent of arriving sea containers.

Ensuring Resilience to Disasters

Read the Implementing 9/11 Commission Recommendations, Progress Report 2011

The Department of Homeland Security (DHS) and its many partners across the federal government, public and private sectors, and communities across the country and around the world have worked since 9/11 to build a new homeland security enterprise to better mitigate and defend against dynamic threats, minimize risks, and maximize the ability to respond and recover from attacks and disasters of all kinds.

Together, these efforts have provided a strong foundation to protect communities from terrorism and other threats, while safeguarding the fundamental rights of all Americans.

While threats persist, our nation is stronger than it was on 9/11, more prepared to confront evolving threats, and more resilient in the face of our continued challenges.

Progress Made Since 9/11

DHS provides the coordinated, comprehensive federal response in the event of a terrorist attack, natural disaster or to other large-scale emergencies while working with federal, state, local, and private sector partners to ensure a swift and effective recovery effort. The Department's efforts to build a ready and resilient nation through a "Whole Community" approach include enhancing emergency communications and interoperability; building nuclear, radiological, and biological preparedness capabilities; and providing grants, plans and training to our homeland security partners. Since fiscal year 2003, DHS has awarded more than $31 billion in preparedness grant funding based on risk, to build and sustain targeted capabilities to prevent, protect against, respond to, and recover from threats or acts of terrorism and natural disasters.

Enhancing Emergency Communication Infrastructure and Improving Interoperability

- **Emergency and Interoperable Communications Plans**: In 2008, the DHS Office of Emergency Communications (OEC) developed the National Emergency Communications Plan in coordination with more than 150 public safety practitioners at all levels of government and across responder disciplines, which serves as the first nationwide strategic plan to improve emergency communications and drive measurable progress.

- **Urban Area Emergency Communications:** In 2010, OEC worked with 60 urban areas to assess emergency communications during a real-world situation. All 60 urban areas successfully demonstrated response-level emergency communications. OEC has also trained more than 3,500 first responders, technicians, and planners to lead communications at incidents across the nation.

- **Virtual USA**: Launched in 2009, this information-sharing system links disparate tools and technologies at all levels of government to share the location and operational status of critical resources through voice, video, geospatial platforms, and imagery with the homeland security and emergency management community.

- **Integrated Public Alert and Warning System**: The Federal Emergency Management Agency (FEMA) is developing the nation's next-generation infrastructure for alert and warning capabilities, known as PLAN (Personal Localized Alerting Network). This new public safety system allows customers with an enabled mobile device to receive geographically-targeted messages alerting them of imminent threats to safety in their area.

Building Nuclear, Radiological, and Biological Preparedness and Response Measures

- **State and Local Radiological Emergency Preparedness**: DHS's Domestic Nuclear Detection Office has trained more than 15,000 state and local officers and first responders in radiological and nuclear detection. In addition, through the Securing the Cities initiative, nearly 11,000 personnel in the New York City region have been trained in preventive radiological and nuclear detection operations and nearly 6,000 pieces of radiological detection equipment have been deployed. The Administration has proposed expanding the Securing the Cities initiative to additional high risk regions of the country.

- **BioWatch**: BioWatch is a federally-managed, locally-operated, nationwide bio-surveillance system designed to detect the intentional release of aerosolized biological agents.

- **Biopreparedness Information Sharing**: To improve state and local biopreparedness, DHS established the first formalized sharing of public health and intelligence information with state and local health partners in 2009. In 2010, the Department developed and conducted a series of biodefense response exercises, including one in each of the 10 FEMA regions, involving more than 1,000 state and local officials.

Private Sector Preparedness

- **Voluntary Private Sector Preparedness Accreditation and Certification Program (PS-Prep™)**: DHS created the PS-Prep™ program, a partnership between DHS and the private sector that enables private entities to receive emergency preparedness certification. Under PS-Prep™, DHS and FEMA adopted three industry standards to assist organizations in assessing their preparedness and resiliency.

- **Ready Campaign**: FEMA promotes private sector preparedness through its Ready Business campaign, a nationwide initiative that provides materials to businesses to encourage continuity planning and crisis management. Ready Business is part of larger preparedness outreach efforts by FEMA that include the Ready campaign and Citizen Corps, to encourage Americans to prepare for emergencies in their homes, businesses, and communities.

- **Risk Mitigation Training:** In total, more than 33,000 state, local and private sector security partners have taken risk mitigation training on a range of topics.

Safeguarding and Securing Cyberspace

Read the Implementing 9/11 Commission Recommendations, Progress Report 2011

The Department of Homeland Security (DHS) and its many partners across the federal government, public and private sectors, and communities across the country and around the world have worked since 9/11 to build a new homeland security enterprise to better mitigate and defend against dynamic threats, minimize risks, and maximize the ability to respond and recover from attacks and disasters of all kinds.

Together, these efforts have provided a strong foundation to protect communities from terrorism and other threats, while safeguarding the fundamental rights of all Americans.

While threats persist, our nation is stronger than it was on 9/11, more prepared to confront evolving threats, and more resilient in the face of our continued challenges.

Progress Made Since 9/11

DHS has made significant strides in enhancing the security of the nation's critical physical infrastructure as well as its cyber infrastructure and networks. Today's threats to cybersecurity require the engagement of the 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.

Analyzing and Reducing Cyber Threats and Vulnerabilities

- **National Cybersecurity Protection System**: Developed by DHS as the nation's focal point for cyber activity and analysis, The National Cybersecurity Protection System fulfills a key requirement of the National Cybersecurity Protection Plan (NCPP) to work collaboratively with public, private, and international entities to protect infrastructure, enhance situational awareness and implement analysis, warning and risk-management programs.

- **EINSTEIN**: Initially deployed in 2004, this system helps block malicious actors from accessing federal executive branch civilian agencies while working closely with those agencies to bolster their defensive capabilities. EINSTEIN 2 is an automated cyber surveillance system that monitors federal internet traffic for malicious intrusions at 15 Departments and agencies and four Managed Trusted Internet Protocol Service providers. EINSTEIN 3 will provide DHS with the ability to detect malicious activity and disable attempted intrusions automatically.

- **Trusted Internet Connections**: As part of the Comprehensive National Cybersecurity Initiative, DHS works to reduce and consolidate the number of external connections that federal agencies have to the Internet in order to limit the number of potential vulnerabilities to government

networks and to focus monitoring efforts and security capabilities on limited and known avenues for Internet traffic.

- **U.S. Computer Emergency Readiness Team (US-CERT)**: In partnership with antivirus companies, US-CERT takes proactive measures to stop possible threats from reaching public and private sector partners by developing and sharing standardized threat indication, prevention, mitigation, and response information products with its .gov partners and constituents.

Distributing Threat Warnings

- **National Cybersecurity and Communications Integration Center**: Opened in October 2009, this 24-hour watch and warning center serves as the nation's principal hub for organizing cyber response efforts and maintaining the national cyber and communications common operational picture. DHS also works with the private sector, other government agencies and the international community to mitigate risks by leveraging the tools, tradecraft, and techniques malicious actors use and converting them into actionable information for all 18 critical infrastructure sectors to use against cyber threats.

- **Cybersecurity Partners Local Access Plan:** DHS enhances information sharing with cleared owners and operators of critical infrastructure and key resources, as well as state technology officials and law enforcement officials, through access to secret-level cybersecurity information and video teleconference calls via local fusion centers.

- **Information Sharing and Analysis Centers:** DHS enhances situational awareness among stakeholders including those at the state and local level as well as industrial control system owners and operators by allowing the federal government to quickly and efficiently provide critical cyber risk, vulnerability, and mitigation data.

Coordinating Response to Cyber Incidents

- **Interagency Collaboration**: In October 2010, DHS and DOD signed a landmark memorandum of agreement to align and enhance America's capabilities to protect against threats to critical civilian and military computer systems and networks while ensuring appropriate levels of privacy.

- **National Cyber Incident Response Plan:** Developed in September 2010, this plan coordinates the response of multiple federal agencies, state and local governments, and hundreds of private firms, to incidents at all levels. DHS tested this plan during the CyberStorm III national exercise, which simulated a large-scale attack on the nation's critical information infrastructure.

Ensuring Safety of Cyber Systems

- **Cybersecurity Workforce Initiative**: Since its creation, DHS has increased its cyber staff by 500 percent while working with universities to build the cybersecurity pipeline through competitive scholarship, fellowship, and internship programs to continue to attract top talent.

- **Technological Development and Deployment**: DHS is guiding research and development as well as advancements in scientific and technical knowledge to support cybersecurity through targeted grant programs that encourage academic research, private sector investment, and innovation from small businesses.

Public Engagement

- **Stop.Think.Connect.**: The Department's **Stop.Think.Connect.** public cybersecurity awareness campaign is designed to increase public understanding of cyber threats and promote simple steps the public can take to increase their safety and security online.

- **National Cybersecurity Awareness Month**: Every October, DHS and its public and private sector partners promote efforts to educate citizens about guarding against cyber threats.

International Engagement

Read the Implementing 9/11 Commission Recommendations, Progress Report 2011

The Department of Homeland Security (DHS) and its many partners across the federal government, public and private sectors, and communities across the country and around the world have worked since 9/11 to build a new homeland security enterprise to better mitigate and defend against dynamic threats, minimize risks, and maximize the ability to respond and recover from attacks and disasters of all kinds.

Together, these efforts have provided a strong foundation to protect communities from terrorism and other threats, while safeguarding the fundamental rights of all Americans.

While threats persist, our nation is stronger than it was on 9/11, more prepared to confront evolving threats, and more resilient in the face of our continued challenges.

Progress Made Since 9/11

DHS works closely with international partners, including foreign governments, major multilateral organizations, and global businesses, to strengthen the security of the networks of global trade and travel upon which the nation's economy and communities rely. DHS has also worked with international organizations on an unprecedented initiative to strengthen global aviation against threats posed by terrorists, working in multilateral and bilateral contexts with governments as well as industry worldwide. The Administration's global supply chain initiative is building on many of these partnerships, including work with International Civil Aviation Organization (ICAO), World Customs Organization (WCO) and International Maritime Organization (IMO).

Cooperation with Mexico and Canada

Secretary Napolitano and her Mexican and Canadian counterparts have signed numerous bilateral agreements and declarations to deepen cooperation and collaboration in the areas of enforcement, planning, information and intelligence sharing, joint operations, and trade facilitation along our borders. In May 2010, Presidents Obama and Calderon issued a Declaration on 21st Century Border Management, pursuing initiatives designed to expedite the legitimate flow of people and goods and focus law enforcement resources on those people and goods that represent the highest risk or about which officials know the least. In February 2011, President Obama and Prime Minister Harper of Canada announced the " Shared Vision for Perimeter Security and Economic Competitiveness," emphasizing shared responsibility for safety and security by addressing threats at the earliest point possible; facilitating trade, economic growth, and jobs; collaborating on cross-border law enforcement; and partnering to strengthen the resilience of critical infrastructure and cybersecurity.

International Partnerships

- **Aviation Security Partnerships:** DHS has enhanced the security of the global aviation system, not only domestically, but also in airports abroad, by working directly with foreign governments, international organizations, and the aviation industry to raise aviation security standards. To date, nearly a dozen countries have deployed or piloted Advanced Imaging Technology in their major airports to screen passengers for metallic and non-metallic threats, including weapons, explosives and other objects concealed under layers of clothing.

- **Biometric Information-Sharing:** DHS and the Department of State have worked with Australia, Canada, New Zealand, and the United Kingdom to develop routine sharing of biometric information collected for immigration purposes.

- **Cargo Screening**: Fulfilling a requirement of the 9/11 Act, 100 percent of high risk cargo on international flights bound for the United States is screened.

- **Container Security Initiative**: The Container Security Initiative, currently operational in 58 foreign seaports through agreements in 32 countries, identifies and screens all U.S.-bound maritime containers that pose a potential risk.

- **Criminal History Information Sharing Arrangement**: The Criminal History Information Sharing Arrangement between the United States and Mexico enables Immigration and Customs Enforcement (ICE) to provide serious felony conviction information on Mexican nationals being repatriated to Mexico.

- **Customs Trade Partnership Against Terrorism (C-TPAT)**: Cargo security throughout the international supply chain is strengthened through this voluntary public-private sector partnership program in which DHS works closely with importers, carriers, licensed customs brokers, and manufacturers. As of May 2011, C-TPAT had more than 10,100 Certified Partners and has conducted more than 17,700 on site validations of manufacturing and logistics facilities in 97 countries, representing some of the highest risk areas of the world.

- **Declaration on Aviation Security**: In October 2010, nearly 190 countries signed a historic ICAO agreement that establishes a foundation for aviation security to better protect the entire global aviation system and make air travel safer and more secure than ever before.

- **Electronic System for Travel Authorization (ESTA)**: Since 2009, nationals from all Visa Waiver Program (VWP) countries, regardless of their port of embarkation, have been required to obtain an approved travel authorization via ESTA, which screens travelers against government databases, prior to boarding a carrier to travel by air or sea to the United States.

- **Federal Air Marshal Service Agreements**: Through such partnerships, U.S. Federal Air Marshals are permitted on international U.S. carrier flights to and from 60 countries.

- **Illegal Drug Program**: In October 2009, ICE launched this effort in Nogales, Ariz. to refer narcotics smuggling cases declined for prosecution in the United States to Mexico for prosecution. In April 2010, ICE expanded this program to El Paso, TX.

- **Immigration Advisory Program**: Arrangements in eight locations enable Customs and Border Protection (CBP) officers posted at foreign airports to use advanced targeting and passenger analysis information to identify high-risk travelers at foreign airports before they board U.S.-bound flights.

- **Integrated Cross-Border Maritime Law Enforcement Operations Shiprider Agreement** *(PDF, 17 pages - 1.2 MB)* In May 2009, the U.S. and Canada signed an agreement enabling law enforcement from both countries to cross-train, share resources and personnel, and utilize each others' vessels in the waters of both countries.

- **Maritime Operations Letter of Intent:** This cooperative effort between the militaries of the U.S. and Mexico was initiated to develop, exercise and execute maritime security and safety standard operating procedures for coordinated bi-national maritime operations.

- **Program Global Shield**: Launched in coordination with the World Customs Organization, this multilateral law enforcement effort works to combat the illicit cross-border diversion and trafficking of precursor chemicals for making improvised explosive devices by monitoring cross-border movements.

- **Pre-Clearance Agreements**: Pre-clearance agreements are in place in Aruba, Bahamas, Bermuda, Canada and Ireland, allowing DHS to screen travelers and their baggage before takeoff through the same process a traveler would undergo upon arrival at a U.S. port of entry to better target and prevent threats while streamlining legitimate travel.

- **Preventing and Combating Serious Crime Agreements**: DHS, in collaboration with the Departments of Justice and State, has signed Preventing and Combating Serious Crime (PCSC) Agreements with 17 Visa Waiver Program countries and one non-VWP country, which enables international partners to query the fingerprint databases of others for law enforcement purposes and voluntarily provide data about criminals and terrorists.

- **Science and Technology Agreements**: DHS has signed 12 international agreements to foster collaboration in science and technology, including research and development in cutting-edge technologies to ensure our mutual security

- **Visa Security Program**: ICE, with support from the Department of State, deploys trained special agents overseas to high-risk visa activity posts to identify potential terrorist and criminal threats before they reach the United States. The Visa Security Program is currently deployed to 19 posts in 15 countries.

- **Visa Waiver Program**: Under this program, nationals from 36 participating countries are able to travel to the United States for stays of 90 days or less upon receiving travel authorization through the ESTA program. The 9/11 Act requires VWP countries to enter into an agreement with the United States to share lost and stolen passport data, as well as terrorism information and information on serious criminal offenses.

- **Western Hemisphere Travel Initiative**: To enhance border security, this effort requires U.S., Mexican and Canadian citizens to present a passport or other secure travel document that denotes identity and citizenship when entering the U.S.

###