

**DEPARTMENT OF HOMELAND SECURITY
PROGRESS IN IMPLEMENTING
9/11 COMMISSION RECOMMENDATIONS
JULY 2010 UPDATE**

GUARDING AGAINST TERRORISM AND ENSURING TRANSPORTATION SECURITY

RECOMMENDATION: Develop a Risk-Based Plan for Transportation Security

Transportation Sector Security Risk Assessment

In June 2010, the Transportation Security Administration (TSA) provided to Congress the Transportation Sector Security Risk Assessment (TSSRA) report, a nationwide risk assessment that examines the potential threat, vulnerabilities, and consequences of a terrorist attack involving the Nation's transportation system. This report will inform the risk-based development and maintenance of risk mitigation strategies and actions that include the development of security standards, grants, programs, countermeasures, and resource allocations.

Freight Railroad Security Risk Assessment

In June 2010, TSA submitted to Congress the Freight Railroad Security Risk Assessment and National Strategy report as required by the 9/11 Act. This report provides the results of a comprehensive assessment of the risk of a terrorist attack involving the Nation's freight railroad transportation system. The report also includes a national strategy for railroad transportation.

Threat Assessment of the Risk of Terrorist Attack on the Nation's School Bus System

In early 2010, TSA submitted to Congress the Threat Assessment of the Risk of Terrorist Attack on the Nation's School Bus System, as required by the 9/11 Act. This report was developed in conjunction with school transportation and school security leaders nationwide, outlining the threats and vulnerabilities this system faces and an analysis of strategies to mitigate risk.

Transportation Security Funding

To support transportation infrastructure and security, the Department of Homeland Security (DHS) provided the following resources to state and local jurisdictions based on risk and threats in Fiscal Year (FY) 2010 and through the American Recovery and Reinvestment Act (ARRA):

- \$403 million for the Transit Security Grant Program to protect critical transit infrastructure from terrorism, including capital projects, such as improvements to high-risk, high-density tunnels, stations, and bridges and law enforcement officers at transit systems across the country. (\$150 million ARRA/ \$253 million FY2010 funding)
- \$1.76 billion for state-of-the-art in-line explosive detection systems to streamline checked baggage screening at airports throughout the U.S. (\$734 million ARRA/ \$1.028 billion FY2010 funding)
- \$14.5 million for the Freight Rail Security Grant Program to protect critical freight rail systems infrastructure from acts of terrorism resulting from railroad cars transporting toxic inhalation hazardous materials.
- \$20 million for Intercity Passenger Rail (Amtrak) to protect critical surface transportation infrastructure and the traveling public from terrorism within the Amtrak rail system.

Additionally, DHS spent \$394 million for the passenger screening through Advanced Technology X-Ray machines, Advanced Imaging Technology machines, bottle liquid scanners, Explosive Trace Detection machines, and other enhanced threat-detection equipment. (\$266 million ARRA/ \$128 million FY2010 funding)

Aviation Security

Fulfilling a key recommendation of the *9/11 Commission Report*, TSA implemented Secure Flight for 100 percent of passengers flying domestically and internationally on U.S. airlines in June of 2010. TSA expects all international carriers with direct flights to the United States to be using Secure Flight by the end of 2010. Under Secure Flight, TSA prescreens passengers directly against government watchlists, a function previously performed by individual air carriers. In addition to facilitating secure travel for all passengers, Secure Flight helps prevent the misidentification of passengers who have names similar to individuals on government watchlists.

Since the attempted terrorist attack on December 25, 2009, Secretary Napolitano, in conjunction with the International Civil Aviation Organization (ICAO), has been leading a global initiative to strengthen the international aviation system against the evolving threats posed by terrorists, working in multilateral and bilateral contexts with governments as well as industry. Over the past six months, Secretary Napolitano has participated in regional aviation security summits around the world, forging historic consensus with her international colleagues to strengthen the civil aviation system through enhanced information analysis and sharing, cooperation on technological development and modernized aviation security standards. These meetings will culminate in the ICAO Triennial Assembly in September where DHS expects member states will affirm new standards, key measures, and proposals for increasing aviation security worldwide.

Domestically, DHS has bolstered security measures at all of our airports, by implementing a variety of security measures to further improve an enhanced, risk-based, layered approach to security. DHS and TSA deploy the most effective technologies available to counter evolving threats, including next generation Explosive Trace Detection units, Advanced Imaging Technology, and next generation Bottled Liquids Scanners. The deployment of over 50,000 trained Transportation Security Officers, Transportation Security Inspectors, and Behavior Detection Officers and 730 canine teams in the transportation sector add additional layers of security to support the technology at the checkpoints

DHS has also strengthened partnerships across the federal government, working with the Department of Justice (DOJ) on a number of initiatives to enhance risk-based aviation security countermeasures and collaborating with the Department of Energy (DOE) and its National Laboratories to leverage their expertise in building risk-based technology solutions to key aviation security challenges.

Further, each year, DHS/TSA conducts international aviation security training for countries around the world focusing on risk-based security strategies, including cargo security, screening technologies, and airport security management, among other topics. TSA has also successfully negotiated agreements with various foreign governments permitting Federal Air Marshal deployments on international U.S. carrier flights, based on risk.

Additionally, air cargo carried on passenger aircraft has never been more secure. Currently, 100 percent of identified high risk international inbound cargo and 100 percent of total cargo on more than 95 percent of all flights originating from U.S. airports are now screened. TSA is on track to meet

the Congressionally-mandated 100 percent screening requirement for all air cargo on domestic passenger aircraft by August 2010.

The FY 2011 DHS budget request strengthens several aviation security programs by allowing increased Federal Air Marshal coverage on international flights and through the deployment of additional canine teams, Behavior Detection Officers, Explosive Trace Detection machines and Advanced Imaging Technology units to increase the Department's ability to detect metallic and non-metallic explosives and other threats at airports across the country.

Surface Transportation Protection

Recognizing that the risk from terrorism and other hazards for surface transportation demands a coordinated approach involving all sector partners and stakeholders, the Administration initiated a thorough review of existing U.S. surface transportation security efforts across all modes of surface transportation in 2009. The resulting Surface Transportation Security Priority Assessment, released on April 2, 2010, identified interagency priorities for the next four years and provided concrete recommendations on how to enhance security efforts, maximize the use of partnerships to optimize public safety, facilitate commerce and strengthen the resiliency of our surface transportation system.

DHS has completed risk-based implementation plans for each of the 20 consensus recommendations of the Surface Transportation Security Priority Assessment addressing the potential risks to the surface transportation system and its four subsectors (mass transit, highways, freight rail, and pipelines), and initiatives are underway.

The Baseline Assessment for Security Enhancement (BASE) program for mass transit provides a comprehensive assessment of the security programming in critical transit systems around the country in order to identify security concerns and drive program priorities and resource allocations.

Additionally, TSA has many programs designed to bolster surface transportation security, including the deployment of Visible Intermodal Prevention and Response (VIPR) Teams, comprised of Federal Air Marshals, surface/aviation transportation security inspectors, Behavioral Detection Officers, Transportation Security Officers, local law enforcement and security personnel, and canine teams, which enhance the protection of surface transportation, provide deterrent and detection capabilities, and introduce an element of unpredictability in security practices and procedures in order to prevent or disrupt potential terrorist planning activities.

Maritime Transportation Security

In January 2010, Customs and Border Protection (CBP) began enforcement of the Importer Security Filing and Additional Carrier Requirements interim final rule—also known as the “10 + 2 rule”—increasing the scope and accuracy of information gathered on shipments of cargo arriving by sea into the United States and bolstering DHS' layered enforcement strategy to protect against terrorism and other crimes at U.S. ports of entry.

In FY 2010, DHS provided \$288 million in grants for the Port Security Grant Program—awarded based on risk—to protect critical port infrastructure from terrorism, enhance maritime domain awareness and risk management capabilities, and support the implementation of the Transportation Worker Identification Credential, and an additional \$150 million in Recovery Act funding.

The United States Coast Guard (USCG) has many risk-based initiatives in place that strengthen maritime transportation security. For example, Operation Neptune Shield, which includes waterborne and aerial patrols as well as armed escorts of hazardous cargos and passenger vessels, helps to reduce the risk of terrorism to the maritime transportation system, critical infrastructure and key resources. The USCG also has developed Advanced Interdiction capabilities in order to interdict identified threats, including chemical, biological, radiological, nuclear, and explosives threats, before they reach the United States. The USCG conducts intelligence-informed, risk-based Security Boardings to verify the identity of crew members and to ascertain if a vessel poses a threat to the port and whether it should be permitted or denied entry.

The USCG also utilizes the Maritime Security Risk Analysis Model, known as MSRAM, to assess threat, vulnerability, and consequence factors for various potential terrorist attack scenarios. This information allows for increased efficiency in the allocation of maritime security resources to reduce security risks at a port. Finally, the USCG's International Port Security Program (PSP) assesses the effectiveness of anti-terrorism measures in foreign ports that conduct maritime trade with the United States and assists in measuring the risk posed by vessels who have visited international ports prior to coming to the United States.

RECOMMENDATION: Improve airline passenger pre-screening

New, More Flexible Screening Measures

On April 8, 2010, DHS began implementing new enhanced security measures for all air carriers with international flights to the United States 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 real-time, threat-based intelligence along with multiple layers of security, both seen and unseen, to more effectively mitigate evolving terrorist threats.

Secure Flight

Fulfilling a key 9/11 Commission recommendation, in June 2010, TSA implemented Secure Flight for 100 percent of passengers flying domestically and internationally on U.S. airlines, meaning that TSA, not the air carriers, vets passengers against government watchlists using passenger name, date of birth, and gender before a boarding pass is issued. This accounts for over 90 percent of all travel to, from, and within the United States. TSA expects to convert all international carriers to Secure Flight by December 2010.

Identifying High-Risk Travelers

To identify high-risk travelers and facilitate legitimate travel, DHS requires airlines flying to the United States from foreign countries to provide Advance Passenger Information (API), which includes basic information such as name, date of birth, citizenship/nationality and passport number, and Passenger Name Records (PNR), which includes the information that travelers provide to airlines when booking their flights, such as itinerary, address, and check-in information.

DHS analysis of passenger data played a critical role in the recent counterterrorism cases against Najibullah Zazi, who pled guilty to plotting to bomb New York subways, David Headley, who pled guilty for his role in the 2008 Mumbai terrorist attacks, and Times Square bombing suspect Faisal Shahzad.

Trusted Traveler Programs

In order to facilitate legitimate travel and effectively deploy screening and security resources, CBP has vetted and enrolled over 780,000 travelers from over 100 countries in four Trusted Traveler Programs: NEXUS, the Secure Electronic Network for Travelers Rapid Inspection (SENTRI), the Free and Secure Trade (FAST) program, and Global Entry. These programs expedite travel for members who voluntarily apply, provide biometric identification, pass extensive vetting, pay a fee, and provide comprehensive data to CBP for rigorous security threat assessment checks.

Pre-clearance Agreements

DHS has five pre-clearance agreements (with Aruba, Bahamas, Bermuda, Canada and Ireland), allowing DHS to screen travelers 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. The preclearance agreements with Aruba, Bermuda and Ireland have been expanded to apply to private aircraft traveling directly to the U.S.

Immigration Advisory Program

DHS has also implemented 9 Immigration Advisory Program (IAP) arrangements in 7 countries, which enable 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. In 2010, DHS signed agreements to establish similar programs at Mexico City International Airport and Paris/de Gaulle International Airport.

RECOMMENDATION: Improve airline passenger explosive screening

TSA continually assesses intelligence and develops countermeasures to enhance its multiple layers of security at airports and onboard aircraft in order to anticipate and mitigate the constantly evolving threats to aviation security. TSA has deployed more than 50,000 Transportation Security Officers, Transportation Security Inspectors, and Behavior Detection Officers across the U.S. and all officers receive extensive advanced explosive training. TSA has also deployed explosive detection technology, including Advanced Technology X-Ray Machines (which enhance the detection capabilities of carry-on bag screening), next-generation Explosives Trace Detection Machines (which improve explosives detection capabilities at airports) and Advanced Imaging Technology Machines (which allow for increased detection of both metallic and non-metallic threats) to airports across the country to detect potential threats.

As noted above, the Recovery Act provided \$266 million, the FY2010 budget provided \$128.7 million, and the President's FY2011 budget request included \$769 million for passenger screening technologies.

RECOMMENDATION: Improve checked bag and cargo screening

Checked Baggage

TSA screens 100 percent of all checked and carry-on baggage for explosives. As noted above, the Recovery Act provided \$734 million and the FY2010 budget provided \$1.028 billion in funding for new, state-of-the-art in-line explosives detection systems and other technology to streamline checked

baggage screening at airports throughout the U.S. and hundreds of next generation explosives trace detection units.

Cargo Screening

Air cargo on passenger aircraft has never been more secure. Currently, 100 percent of identified high risk international inbound cargo and 100 percent of total cargo on more than 95 percent of all flights originating from U.S. airports are now being screened.

TSA is on track to meet the Congressionally-mandated 100 percent screening requirement for all air cargo on domestic passenger aircraft by August 2010. Effective May 1, 2010, 75 percent of cargo on passenger aircraft departing from U.S. locations are screened under TSA security programs, largely through the Certified Cargo Screening Program, which permits entities who have undergone rigorous inspection and certification processes throughout the air cargo supply chain to screen cargo. Currently, there are over 1.5 million shippers in TSA's Known Shipper Management System that have been certified as meeting specific security standards.

Port Security

CBP has deployed Radiation Portal Monitors and other radiation detection technologies to seaports, land border ports, and mail facilities around the world. These systems scan 100 percent of all containerized cargo arriving in the U.S., including 100 percent of vehicles arriving through our southern border ports, over 99 percent of arriving sea containers, 100 percent of trucks and 100 percent of personal vehicles arriving at our northern border ports.

DHS has also implemented the Secure Freight Initiative to scan U.S.-bound maritime containers for nuclear material overseas and the Container Security Initiative to ensure that all U.S.-bound maritime containers that pose a potential risk are identified and inspected before they are placed on vessels destined for the U.S.

Canine Teams

Canine teams are an integral part of DHS's layered approach to baggage and cargo security and are deployed by TSA, CBP and USCG in their respective environments. CBP deploys canine detection teams at and between ports of entry, expediting inspections along the border to combat terrorist threats and interrupt the illegal smuggling of drugs, currency, firearms, humans, and agricultural products. TSA deploys canine teams to screen air cargo at the nation's highest cargo volume airports and provide explosives detection capabilities in the aviation, mass transit, and maritime transportation sectors. Finally, USCG deploys canine explosive detection teams to strategic U.S. ports to enhance security throughout the maritime transportation sector. The Recovery Act provided \$150 million for the Transportation Security Grant Program, of which \$78 million is being used by transit agencies to hire new law enforcement officers and by police departments with dedicated transit bureaus to hire anti-terrorism personnel, purchase anti-terrorism equipment, and obtain and train explosive detection canines.

Nuclear Detection

DHS's Domestic Nuclear Detection Office (DNDO) works to improve the Nation's capability to detect and report unauthorized attempts to import, develop, or transport nuclear or radiological material for use against the U.S. DNDO has worked with intra- and inter-agency partners to develop strategies for improving the probability of detecting and interdicting radiological and nuclear threats. Since its inception, DNDO has launched more than 250 research and development projects

with National Laboratory, academic, and industrial partners, aimed at advancing detection technologies. DNDO has also made radiological and nuclear detection training available to over 15,000 state and local officers and first responders. In order to meet the challenge of the global helium 3 shortage, DNDO is aggressively bringing alternative technologies for helium 3 from concept to product through a rapid acquisition process, expediting new and innovative detection technology.

DNDO works across DHS to develop nuclear detection capabilities throughout the transportation sectors. TSA's VIPR Program is currently working in conjunction with DNDO and DOE and has the capability to deploy preventative radiological and nuclear detection equipment to the field. CBP has deployed hundreds of Radiation Portal Monitors to ports of entry, airports and seaports to screen cars, trucks, and other conveyances for the presence of radioactive and nuclear materials. Finally, all USCG teams are now equipped with radiation detection capabilities, including USCG personnel specifically trained to board and search vessels.

In March 2010, DHS renewed a Project Arrangement "Concerning the Detection of Illicit Movement of Radiological and Nuclear Materials" with the U.K. to address information and data sharing between the countries in the development of radiation and nuclear detection equipment and technology.

RECOMMENDATION: Vigorously track and disrupt terrorist financing

Disrupting terrorist financing is one of a number of tools that the U.S. Government employs to counter terrorism. The Secret Service has expanded its Electronic Crimes Task Force (ECTF) program across the country and internationally, with its first international ECTF in Rome, Italy. These task forces are designed to prevent, detect, and investigate various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems. Additionally, the Secret Service has Special Agents assigned to all Joint Terrorism Task Forces around the country. These locally-based facilities partner federal, state and local law enforcement and intelligence agencies to target and prevent terrorist activities.

Furthermore, Immigration and Customs Enforcement (ICE) has a lead role in combating bulk cash smuggling, a common strategy used by criminals seeking to move illicit proceeds across transnational borders. ICE's Operation Firewall, a bulk-cash smuggling initiative that intercepts currency smuggling en route to the border, has led to more than hundreds of arrests and the seizure of more than \$316 million, including \$116 million seized overseas. ICE has provided outreach and training on the interdiction and investigation of bulk currency violations to more than 2,500 law enforcement, financial, and government officials in more than 85 countries.

ICE also developed the Cornerstone Initiative to detect and close gaps within U.S. financial, trade, and transportation sectors that can be exploited by criminal networks, and ICE's Trade Transparency Units target money laundering and illegal trade transactions. These Trade Transparency Units have launched over 600 trade-based money laundering investigations, seizing more than \$180 million since 2004.

SECURING OUR BORDERS

RECOMMENDATION: Standardize secure identification

DHS strongly supports national standards for identification documents to strengthen security while enhancing privacy safeguards. Over the past several years, DHS has taken numerous steps to implement this recommendation to help prevent terrorism, reduce fraud, and improve the reliability and accuracy of personal identification documents.

Western Hemisphere Travel Initiative (WHTI)

In June 2009, DHS successfully implemented the Western Hemisphere Travel Initiative (WHTI) for land and sea travel to the U.S., increasing border security while facilitating legitimate travel and trade by requiring that U.S. and Canadian citizens present a passport or other secure travel document that denotes identity and citizenship when crossing the border.

In response to WHTI, CBP is working with tribes across the country on the development of Enhanced Tribal Cards (ETC)—WHTI compliant documents that formally recognize tribal membership and U.S./Canadian citizenship for the purpose of border crossing. To date, CBP has signed Memorandum of Agreements for the development of ETCs with the Kootenai Tribe of Idaho, the Pascua Yaqui of Arizona, the Tohono O’Odham of Arizona, the Seneca Nation of New York, and the Coquille of Idaho, and is working with additional tribes on the ETC initiative.

Drivers License Security

Under DHS’s Driver’s License Grant Security Grant Program, states have made substantial progress in improving the security and integrity of their driver’s licenses and issuance processes. Over the past 3 years, this program has provided \$176.4 million to states to assist with implementing these security procedures.

DHS continues to work with states and territories, congressional allies, and the National Governors Association to enhance the security of driver’s licenses while reforming and resolving many of the concerns in the REAL ID Act through legislation.

Transportation Worker Identity Credential (TWIC) Program

DHS has enrolled over 1.6 million port workers and merchant mariners in the Transportation Worker Identity Credential (TWIC) program, a tamper-resistant biometric credential issued to those who require unescorted access to secure areas of ports and vessels.

Citizenship and Immigration Documents

In May 2010, U.S. Citizenship and Immigration Services (USCIS) launched a new card personalization system with state-of-the-art technology that enhances the verification and sharing of electronic records. USCIS redesigned all of its secure identity documents to comport with the latest DHS and International Civil Aviation Organization (ICAO) standards, as well as best practices in industry and government.

The new Permanent Resident Card (“green card”) includes a radio frequency identification tag that allows CBP 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. Additionally, USCIS updated the Employment Authorization Document by adding a machine-

readable zone that for the first time allows USCIS to share data through these work authorization cards with CBP and U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT).

RECOMMENDATION: Integrate border security into larger network of screening points that includes the transportation system and access to vital facilities

Biometric Entry-Exit Screening System

The US-VISIT biometric identity and verification process collects digital fingerprints and a photograph from international travelers at U.S. visa-issuing post and ports of entry to help immigration officers determine whether a person is eligible to receive a visa or enter the United States. US-VISIT also supports the Department's ability to identify international travelers who have remained in the United States beyond their period of admission. To date, DHS has achieved ten-fingerprint collection at entry for 98 percent of inbound travelers.

Visa Waiver Program and Lost and Stolen Passport Screening

The Visa Waiver Program (VWP) enables nationals of 36 participating countries to travel to the United States for tourism or business for stays of 90 days or less without obtaining a visa. DHS implemented the Electronic System for Travel Authorization (ESTA) to screen VWP applicants prior to travel to the United States and, as a result, has virtually eliminated the paper arrival/departure form (Form I-94W) for authorized travelers from nations participating in the VWP.

DHS—in cooperation with the Departments of State and Justice—has made substantial progress in bringing VWP countries into compliance with the information sharing requirements of the 9/11 Act. The 9/11 Act requires VWP countries to enter into an agreement with the United States to report lost and stolen passport data to the United States so that it can be screened against INTERPOL's Stolen and Lost Travel Document database, which contains the lost and stolen passport records of more than 120 countries. To date, 32 of the 36 VWP countries have reached such agreements.

In addition, DHS, in collaboration with the Departments of Justice and State, has signed Preventing and Combating Serious Crime (PCSC) Agreements with 14 VWP countries to share information to better identify known terrorists and criminals during investigations and other law enforcement activities.

Visa Security Program (VSP)

DHS is expanding the Visa Security Program (VSP) to U.S. Embassies and Consulates identified by the Departments of State and Homeland Security as having the highest risk from a terrorism perspective, subject to appropriations and Departmental approval. DHS provides expert advice and training to consular officers regarding specific security threats relating to the adjudication of individual visa applications; reviews applications; and conducts investigations with respect to consular matters under the jurisdiction of DHS.

Southwest Border

Southwest Border Initiative

In March 2009, the Obama Administration announced the Southwest Border Initiative—a series of unprecedented steps to crack down on Mexican drug cartels by deploying additional personnel and

technology, increasing information sharing, working closely with the Mexican government, and improving federal coordination with state, local and tribal law enforcement authorities.

Over the past sixteen months, DHS has dedicated unprecedented personnel, technology, and resources to the Southwest border. Today, the Border Patrol is better staffed than at any time in its 85-year history, having nearly doubled the number of agents from approximately 10,000 in 2004 to more than 20,000 today. Since March 2009, DHS has doubled the number of personnel assigned to Border Enforcement Security Task Forces; tripled the number of ICE intelligence analysts working along the U.S.-Mexico border; quadrupled deployments of Border Liaison Officers; and begun screening 100 percent of southbound rail shipments for illegal weapons, drugs, and cash – for the first time ever. DHS has also deployed additional canine teams trained to detect drugs and weapons and non-intrusive inspection technology that help identify anomalies in passenger vehicles at the Southwest Border.

CBP has also worked closely with the Federal Aviation Administration (FAA) to obtain Certificates of Authorization (COA) to operate Unmanned Aerial Systems (UAS), extending surveillance capability to personnel on the ground. The latest COA approvals have increased the miles of airspace available for UAS operations above Texas, enabling CBP to deploy its unmanned aircraft from the eastern tip of California, across the land borders of Arizona, New Mexico, and Texas, and into the maritime border just short of the Texas and Louisiana border.

These initiatives and investments have yielded impressive results. Seizures of contraband along the Southwest border have increased across the board and illegal crossings continue to decline. In 2009, DHS seized over \$39.2 million in southbound illegal currency—an increase of more than \$29.4 million compared to 2008. In total, DHS seized more than \$103 million, 1.7 million kilograms of drugs, and 1,400 firearms in 2009—an increase of more than \$47 million, 450,000 kilograms of drugs, and 300 firearms, respectively, compared to 2008. Additionally, overall apprehensions of illegal aliens decreased from 723,825 in FY2008 to 556,041 in FY2009, a 23 percent reduction, indicating that fewer people are attempting to illegally cross the border.

To continue to bolster these efforts, President Obama recently requested \$600 million in supplemental funds for enhanced border protection and law enforcement activities, and announced the deployment of up to 1,200 National Guard Troops to the Southwest border to contribute additional capabilities and capacity to assist law enforcement agencies.

Interagency Efforts

In June 2009, the Obama Administration released its Southwest Border Counternarcotics Strategy, which provides the Administration's overarching framework to address the threats posed by the illicit narcotics trade along the Southwest border. DHS has also forged historic agreements with DOJ, increasing coordination between ICE and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) 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.

DHS and the Office of National Drug Control Policy (ONDCP) are also partnering to develop and implement Project Roadrunner, an integrated license plate reader recognition system which will target both north- and southbound drug trafficking and associated illegal activity along the Southwest

border. Under this partnership, ONDCP will provide DHS with previously-purchased fixed and mobile cameras—expanding DHS’ existing capabilities at minimal cost.

Collaboration with State and Local Law Enforcement

The federal government has worked closely with state and local law enforcement along the border—leveraging the resources and capabilities of over 50 law enforcement agencies to crack down on transnational criminal organizations.

DHS has increased the funding state and local law enforcement can use to combat border-related crime through Operation Stonegarden—a DHS grant program designed to support state, local, and tribal law enforcement efforts along the border. Based on risk, cross-border traffic and border-related threat intelligence, nearly 83 percent of 2009 and 2010 Operation Stonegarden funding went to Southwest border states.

DHS is also forging a new partnership with major law enforcement associations to create the “Southwest Border Law Enforcement Compact”—designed to boost law enforcement at the border by enabling non-border state and local law enforcement agencies to detail officers to Southwest border state and local law enforcement agencies to focus on criminal networks operating along the border.

Further, ICE is expanding the Joint Criminal Alien Removal Task Forces, comprised of ICE officers and local law enforcement agents who work together to identify and arrest convicted criminal aliens and deploying additional officers to work with state and local jails that are within 100 miles of the Southwest border to ensure the identification of all removable convicted criminal aliens who pose a danger to public safety.

Additionally, DHS is strengthening the analytic capability of fusion centers across the Southwest border to receive and share threat information, and is working with DOJ to create a new system that will link the information systems of all state, local and tribal law enforcement entities operating along the Southwest border, as appropriate, with federal law enforcement.

Finally, DHS is establishing a suspicious activities reporting program for the Southwest border. This will help local law enforcement officers on the front lines recognize and track incidents related to criminal activity by drug traffickers, integrate disparate information from across the border to identify trends and utilize this information for targeted law enforcement operations on both sides of the border.

Increased Cooperation with Mexico

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

For the first time in history, U.S. Border Patrol agents are coordinating joint operations along the Southwest border with Mexican Federal Police, and working together to prosecute human trafficking cases. In addition, the Department is increasing joint training programs with Mexican law enforcement agencies—focusing on money laundering and human trafficking investigations. ICE will

begin training Mexican customs investigators in August 2010, enabling Mexican Customs to support ICE investigations.

To increase information sharing, the United States and Mexico are establishing a new cross-border communications network, which will improve incident response and coordination among participating federal, state, local, and tribal law enforcement and public safety personnel along the border. Additionally, ICE and the Government of Mexico have entered into a Criminal History Information Sharing Agreement in which ICE provides serious felony conviction information on Mexican nationals being repatriated to Mexico.

In October 2009, ICE launched the Illegal Drug Program in Nogales, Arizona to refer narcotics smuggling cases declined for prosecution in the United States to the Mexican Office of the Attorney General for prosecution. In April 2010, ICE expanded this program to El Paso, Texas. DHS is expanding the program to four additional Southwest border ports of entry—for a total of six locations.

In order to help define and ultimately disrupt the movement of criminal proceeds from the United States to Mexico, the Office of Counternarcotics Enforcement, ICE, and the Government of Mexico for the first time ever collaborated in April 2009 on the Bi-National Criminal Proceeds Study, which describes the criminal proceeds supply chain and quantifies important indicators of this illegal financial network.

Northern Border and Increased Cooperation with Canada

DHS has made critical security improvements along the Northern border, investing in additional Border Patrol agents, technology, and infrastructure. By the end of 2010, DHS will have more than 2,200 agents on the Northern border, a 700 percent increase since 9/11. DHS is also deploying technology, including thermal camera systems, Mobile Surveillance Systems, and a Remote Video Surveillance System, to the Northern border, and is using Recovery Act funds to modernize 29 CBP-owned land ports of entry along the Northern border to meet the security and operational standards of our post-9/11 world.

In May 2009, Secretary Napolitano signed the Shiprider Agreement with Canada to make joint law enforcement teams permanent along the international maritime border. In November 2009, Secretary Napolitano and Public Safety Canada Minister Peter Van Loan agreed on a series of initiatives to combat common threats, including measures to streamline border shipping, assist one another during emergencies, and recognize NEXUS and FAST trusted traveler program cards at all land and sea border ports of entry. Additionally, investigators and intelligence analysts from DHS, the Canada Border Services Agency, and the Royal Canadian Mounted Police share information and analysis through Integrated Border Enforcement Teams and Border Enforcement Security Teams along the border.

In July 2010, Secretary Napolitano and Canadian Minister of Public Safety Vic Toews announced the first-ever U.S.-Canada Joint Critical Infrastructure Action Plan, enabling both countries to more effectively address a range of cross border critical infrastructure issues and work together to share information, identify interdependencies and conduct exercises. They also announced the ICE, CBP, and Canada Border Services Agency currency seizure Memorandum of Understanding, which will help law enforcement officials and border services officers better identify potential threats and assist in money-laundering and terrorist-financing investigations and prosecutions. They also announced a

joint border threat and risk assessment to ensure a common understanding of the threats and challenges, which will enable a coordinated approach to addressing them.

STRENGTHENING PREPAREDNESS EFFORTS

RECOMMENDATION: Allocate homeland security funds based on risk

DHS uses risk-based methodology to identify areas eligible for homeland security grants, accounting for threats, population, economic output, and prevalence of critical infrastructure. In FY2010, DHS awarded the following security grants to assist state, local, and tribal governments and the private sector in strengthening preparedness for acts of terrorism, major disasters, and other emergencies based on risk:

- \$842 million for the State Homeland Security Program to build and strengthen preparedness capabilities at all levels through planning, equipment, and readiness.
- \$832 million for the Urban Areas Security Initiative to enhance urban preparedness capabilities in 64 high-threat, high-density areas, with the seven highest risk areas (Tier 1) receiving 61 percent of available funds.
- \$541 million and an additional \$300 million in Recovery Act funds for Port and Transit Security Grant Programs to create a sustainable, risk-based effort to protect critical infrastructure from terrorism.
- \$48 million for the Interoperable Emergency Communications Grant Program for planning, training, exercises and equipment to states, territories, and local and tribal governments to carry out initiatives identified in Statewide Communication Interoperability Plans.
- \$60 million for the Operation Stonegarden Grant Program to enhance law enforcement preparedness and operational readiness along the border. Based on risk, cross-border traffic and border-related threat intelligence, nearly 80 percent of the funding went to the Southwest border states.

In addition to these grant programs, the Science and Technology Directorate published the 2010 Bioterrorism Risk Assessment (classified) in January of 2010 to inform all federal decision-making about resource allocation and risk management regarding homeland security, infrastructure protection, detectors (such as BioWatch sensors) countermeasures, response plans, and overall consequence management capabilities.

RECOMMENDATION: Improve interoperable communications at all levels of government

DHS has implemented multiple programs to improve interoperable communications across the Department. As noted above, DHS awarded \$48 million through the Interoperable Emergency Communication Grant Program in FY 2010 to fund state and local activities that assist in the implementation of the National Emergency Communications Plan and the Statewide Communication Interoperability Plans.

The Science and Technology Directorate (S&T) is in the final stages of testing the Multi-Band Radio, a portable radio that enables emergency responders to communicate with partner agencies regardless of radio band.

USCG is in the process of establishing Interagency Operations Centers throughout the nation's ports by deploying the Rescue 21 coastal command, control, and communications system and the Watchkeeper information sharing and operational planning and coordination system. The USCG has also developed Mobile Command Center capability, which consists of two Enhanced Mobile Incident Command Posts positioned on each coast, providing robust, interoperable communications anywhere in the world.

As mentioned above, as part of the effort to improve international interoperable communications, the United States and Mexico are establishing a new cross-border communications network, which will improve incident response and coordination among participating federal, state, local, and tribal law enforcement and public safety personnel along the border. Additionally, the Federal Emergency Management Agency (FEMA) is currently developing the nation's next-generation infrastructure of alert and warning capabilities, the Integrated Public Alert and Warning System, which will expand to new mediums of communication.

RECOMMENDATION: Establish a unified incident command system

DHS has incorporated the Incident Command System and National Response Framework into the National Incident Management System, which provides nationwide guidelines to clarify the roles of federal, state and local governments, nongovernmental organizations, and the private sector in protecting against, responding to and recovering from disasters. The response to the BP Deepwater Horizon Oil Spill—which spans all levels of government and includes the private sector—is an example of the implementation of this program, as it has been organized according to the Incident Command System to allow a unified, coordinated response under the leadership of the Department with the Coast Guard as the lead agency. DHS also developed the Unified Incident Command and Decision Project to share information and enhance multi-agency incident command systems and coordination.

RECOMMENDATION: Prioritize private sector preparedness

As part of our commitment to increase private sector preparedness, in June 2010, DHS announced the adoption of the final standards for the Voluntary Private Sector Preparedness Accreditation and Certification Program (PS-Prep)—a major milestone in DHS's implementation the 9/11 Commission's recommendation to create a program to improve private sector preparedness for disasters and emergencies.

RECOMMENDATION: Assess critical infrastructure and readiness

In 2009, DHS revised the National Infrastructure Protection Plan (NIPP), to integrate the concepts of resiliency and protection, and broaden the focus of NIPP-related programs and activities to an all-hazards environment. In FY2010, DHS has provided the following Infrastructure Protection Program grants:

- \$541 million and an additional \$300 million in Recovery Act funds for Port and Transit Security Grant Programs to create a sustainable, risk-based effort to protect critical infrastructure from terrorism.
- \$48 million for the Buffer Zone Protection Program to increase prevention and protection capabilities of law enforcement agencies responsible for safeguarding critical infrastructure such as chemical facilities and nuclear power plants.
- \$11 million for the Intercity Bus Security Grant Program to support security plans, facility security upgrades, and vehicle and driver protection.

DHS is also implementing the Chemical Facility Anti-Terrorism Standards to regulate national security at high-risk chemical facilities. To date, over 38,000 facilities have submitted data on their chemical holdings, and approximately 7,000 have been assessed for risk. The Department has also deployed Protective Security Advisors to all 50 states and Puerto Rico to support state, local, tribal and territorial officials and the private sector with critical infrastructure security efforts and to maintain effective information sharing and situational awareness. Additionally, USCG's Maritime Security Risk Analysis Model has assessed over 22,000 potential terrorist targets spanning 13 critical infrastructure sectors.

DHS also develops an annual National Risk Profile that provides an all-hazards assessment of risks facing critical infrastructure, including terrorist threats, cyber risks, and natural disasters.

In November 2009, DHS launched a new Web site—dhs.gov/criticalinfrastructure—to inform the public about the Department's critical infrastructure protection, readiness and resiliency efforts, part of an increased effort to heighten awareness about the importance of protecting America's vital assets, systems and networks.

PROTECTING PRIVACY AND CIVIL LIBERTIES

RECOMMENDATION: Safeguard Individual Privacy When Sharing Information

DHS involves its Office for Civil Rights and Civil Liberties and the Privacy Office from the outset of the policymaking process, building in rights and liberties protections to new security measures from the beginning. The DHS Privacy Office works to ensure privacy is protected when personally identifiable information is collected, used, shared, or maintained by the Department, and supports U.S. Government-wide policy initiatives governing information sharing by conducting Privacy Impact Assessments of information sharing systems.

The Office for Civil Rights and Civil Liberties and the Privacy Office provide training on civil rights and civil liberties and privacy to intelligence analysts and state and local fusion center personnel. The DHS Privacy Office also supports the Fusion Center Program by reviewing fusion center privacy policies to ensure they adhere to the Information Sharing Environment Privacy Guidelines, participating in the creation of the DHS Joint Fusion Center Program Management Office, and providing training to the Interagency Threat Assessment and Coordination Group.

RECOMMENDATION: Maintain Civil Liberties While Protecting Security

As noted above, DHS involves the Office for Civil Rights and Civil Liberties from the outset of the policymaking process, building in protections to new security measures through collaboration with communities and stakeholders across the country. The DHS Office for Civil Rights and Liberties created a Civil Liberties Impact Assessment process to review Departmental programs, and conduct regular outreach with American Arab, Muslim, Sikh, South Asian, and Somali community leaders, elected officials, and NGOs across the country. Recently, DHS has consulted with privacy, civil rights, and civil liberties advocates about how to build privacy and civil liberties protections into Advanced Imaging Technology, and its operating policies.

DHS is working with communities across the country on preventing violent crime motivated by ideology and on leveraging successful models like community policing. In Summer 2010, DHS and DOJ will launch the “Building Communities of Trust” initiative to enhance local efforts to understand and mitigate the threats facing communities.

These efforts include a public education element through the expansion of the “See Something Say Something” campaign—a simple and effective program to raise public awareness of indicators of terrorism, crime and other threats and emphasize the importance of reporting suspicious activity to the proper transportation and law enforcement authorities. This program was originally implemented by New York City's Metropolitan Transit Authority and was funded, in part, by \$13 million from DHS' Transit Security Grant Program.

IMPROVING COLLABORATION AND INFORMATION SHARING

RECOMMENDATION: Provide Incentives for Information Sharing

Cybersecurity

In October 2009, DHS opened the new National Cybersecurity and Communications Integration Center—a 24-hour, DHS-led coordinated watch and warning center to improve national efforts to address threats and incidents affecting the nation's critical information technology and cyber infrastructure.

Tailoring Information Sharing to State, Local, Tribal and Territorial Customers

DHS, working closely with the FBI, has re-focused its information sharing and production efforts to better address the needs of state, local, tribal, and territorial governments. DHS continually works with senior law enforcement officials from the largest metropolitan areas, the directors of fusion centers, and State Homeland Security Advisors to tailor the Department's efforts, particularly information sharing initiatives, to better support the efforts of state, local, tribal, and territorial law enforcement to protect local communities.

State and Major Urban Area Fusion Centers

DHS supports state and major urban area fusion centers across the country, which share information and intelligence within their jurisdictions as well as with the federal government. To date, 72 state and major urban area analytic centers have been designated as fusion centers by state and local authorities throughout the country. DHS has deployed Homeland Security Data Network (HSDN) systems to the state and major urban area fusion centers, enabling the federal government to share

information and intelligence – including classified terrorism-related threat information – with state, local, tribal, and territorial partners. DHS has also placed federal Intelligence Officers at state and major urban area fusion centers, who act as the primary liaison between the federal governments and state, local, tribal, and territorial partners.

Nationwide Suspicious Activities Reporting Initiative

DHS, in conjunction with DOJ, is also working to implement the Nationwide Suspicious Activities Reporting Initiative (NSI) across the nation. The NSI provides the foundation for state and local efforts to identify and mitigate emerging terrorism related threats through training, reporting and analysis while ensuring privacy and civil liberties are protected. Currently, NSI capability exists in three states (New York, Florida, and Virginia), and nine major cities (Boston, District of Columbia, Chicago, Los Angeles, Las Vegas, Houston, Phoenix, Seattle, and Miami-Dade). Twelve additional states are expected to implement NSI by Fall 2010.

These efforts include a public education element through the expansion of the “See Something Say Something” campaign—a simple and effective program to raise public awareness of indicators of terrorism, crime and other threats, and emphasize the importance of reporting suspicious activity to the proper transportation and law enforcement authorities. The program was originally implemented by New York City's Metropolitan Transit Authority and was funded, in part, by \$13 million from DHS' Transit Security Grant Program.

Improved Analysis of Travel-Related Data

DHS, in partnership with the National Counterterrorism Center and other federal entities, has expanded efforts to analyze travel related data in order to better understand the travel patterns of known and suspected terrorists. Leveraging threat-related intelligence, travel-related data has been essential in identifying, targeting, and interdicting known and suspected terrorists prior to entering the United States or boarding a flight bound for the United States.

First Responders Community of Practice

In April 2010, DHS launched the First Responders Community of Practice, which allows law enforcement, emergency medical services, and emergency management personnel to share best practices and solutions with other professionals, enabling them to more efficiently and effectively prepare for disasters.

QHSR AND THE BOTTOM UP REVIEW

In February 2010, the Department of Homeland Security published our Nation's first ever comprehensive review of America's strategy for homeland security—the Quadrennial Homeland Security Review (QHSR). The QHSR was the first step in setting the strategic path forward to guide the activities of the homeland security enterprise toward a common end: a homeland that is safe, secure, and resilient against terrorism and other hazards. The QHSR identified five core mission areas of homeland security—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.

A bottom-up review (BUR) of the Department of Homeland Security was initiated in November 2009 as an immediate follow-on and complement to the QHSR. The BUR resulted in a comprehensive

catalogue of DHS activities across the homeland security missions. The BUR Report distills the results of this analysis, describing the alignment of the Department and setting forth the Department's priority initiatives and enhancements to increase mission performance, improve Departmental management, and increase accountability over the next four years.

The Department's FY 2012 budget request will begin the process of implementing the BUR initiatives and enhancements, and the corresponding FY 2012-2016 Future Years Homeland Security Program will set forth the budget plan required to provide sufficient resources to successfully execute the Department's responsibilities across the full range of homeland security missions as described in the QHSR, with a priority placed on the initiatives and enhancements set forth in the BUR Report.

###