Homeland Security

Fact Sheet: U.S. Department of Homeland Security 9/11 Anniversary Progress and Priorities

SHARE

Release Date: September 10, 2008

For Immediate Release
Office of the Press Secretary
Contact: 202-282-8010

Since 9/11, the Department of Homeland Security (DHS) has made significant progress in protecting the nation from dangerous people and goods, protecting the nation's critical infrastructure on which our lives and economy depend, strengthening emergency response and unifying department operations. Seven years without an attack on U.S. soil are a testament to this department's 216,000 employees – and the nation's first responders and law enforcement officers – who every day put service before self. Since its creation in the aftermath of the tragic events of 9/11, the department has achieved much to protect and secure the United States:

Protecting the Nation from Dangerous People

DHS prevents the entry of terrorists and criminals while facilitating the legitimate flow of people by strengthening interior security efforts and continuing to increase security at America's borders.

Expanded Border Fencing and Patrol: U.S. Customs and Border Protection (CBP) has completed more than 338 miles of fencing, with approximately 184.2 miles of primary pedestrian fence and approximately 153.8 miles of vehicle fence now in place. CBP is well on its way to the goal of 670 miles of fencing by the end of 2008: 370 miles of pedestrian and 300 miles of vehicle fencing. Additionally, the FY 2009 budget seeks to hire, train and equip 2,200 new Border Patrol agents, which will more than double the size of the Border Patrol from 2001 levels, to 20,000 agents by the end of September 2009.

Connecting the Dots: DHS renewed its Passenger Name Record (PNR) agreement with the European Union, which requires airlines to provide DHS with PNR data for all flights carrying passengers into and out of the U.S. In addition, DHS began accepting voluntary applications on Aug. 1 for the Electronic System for Travel Authorization, a new online system that is part of Visa Waiver Program (VWP) reforms and is required by the Implementing Recommendations of the 9/11 Commission Act of 2007. Once ESTA is mandatory, all nationals or citizens of VWP countries who plan to travel to the U.S. under the VWP will need to receive an electronic travel authorization prior to boarding a U.S.-bound airplane or cruise ship. Rather than relying on paper-based procedures, ESTA will leverage 21st century electronic means to obtain basic information about who is traveling to the U.S.

Better Biometrics: Biometric collection is underway at 106 airports, 15 seaports and in the secondary inspection areas of 154 land ports of entry. Ten U.S. airports currently collect 10 fingerprints from arriving foreign visitors. This transition from two-fingerprint collection enables DHS to check visitors' full set of fingerprints against latent fingerprints collected from terrorist training camps, safe houses and battlefields around the world, without slowing process times – due to the department's work with industry to improve the quality and speed of fingerprint capture devices. Additionally, US-VISIT and the U.S. Coast Guard have partnered to use mobile biometric collection to identify migrants and smugglers attempting to illegally enter the United States through waters near Puerto Rico and the Florida Straits. The program has resulted in a total of 3,143 people interdicted at sea, 172 brought ashore for prosecution – with 143 convicted so far – and a 40 percent reduction in the flow illegal migration.

Secure Documentation Standards: Compliance with Western Hemisphere Travel Initiative requirements for air travel implemented in January 2007 exceeds 99 percent and DHS will implement requirements for land and sea travel in June 2009. New procedures at land and sea ports of entry implemented in January 2008 ended acceptance of oral declarations alone and limited the types of acceptable documents to further secure our borders. DHS also issued the REAL ID final rule, establishing minimum standards that enhance the integrity and reliability of state-issued driver's licenses and identification

cards.

Enhanced Aviation Security: The Transportation Security Administration (TSA) has over 2,000 Behavior Detection Officers working at more than 150 of the nation's largest airports to identify potentially high-risk passengers in airports. Further, TSA now requires that holders of airport-issued identification credentials be perpetually vetted against the Terrorist Screening Database and has expanded its Travel Document Checking program at passenger security checkpoints. TSA also recently achieved DHS certification for the Secure Flight program – through which TSA will assume responsibility from airlines for watch list checking – and anticipates initial implementation in 2008. In October 2005, TSA reclassified the agency's 43,000 screeners as Transportation Security Officers, to acknowledge the judgment and skills required to ensure the safe travels of two million people every day.

New Checkpoint Experience: TSA revamped its airport screening operations, introducing Checkpoint Evolution, at Baltimore in April 2008, which adds a human element to security, and significant technology and process improvements. This continues the agency's shift from object-based security to people-based initiatives, including: whole body imaging; fostering a calm atmosphere in order to better identify suspicious individuals; and advanced technology x-ray to more quickly and efficiently screen carry-on luggage.

Record-Breaking Law Enforcement: So far this year, U.S. Immigration and Customs Enforcement (ICE) has removed or returned more than 295,000 illegal aliens from the U.S. and dramatically increased penalties against employers whose hiring processes violate the law, securing fines and judgments totaling in the millions, while making 1,070 criminal arrests and more than 4,700 administrative arrests. ICE has arrested more than 10,000 gang members and associates in cities nationwide through Operation Community Shield. Through Operation Predator, a program targeting sexual predators that prey on children, ICE has arrested more than 11,000 predators since its inception in 2003. Under DHS, the U.S. Secret Service has made more than 29,000 criminal arrests for counterfeiting, cyber and other financial crimes, 98 percent of which resulted in convictions, and seized more than $295 million in counterfeit currency. Also, in fiscal 2007, the Coast Guard interdicted over 6,000 migrants attempting to gain illegal entry into the U.S.

Protecting U.S. and World Leaders: The Secret Service continues to meet unprecedented challenges of protecting U.S. and world leaders, as well as presidential candidates, while implementing comprehensive plans for securing the overall 2008 presidential campaign. Under DHS, the Secret Service has led the security planning and implementation for more than 10 designated National Special Security Events, including the 2008 Democratic and Republican National Conventions.

E-Verify: This U.S. Citizenship and Immigration Services program allows employers to use an automated system to verify name, date of birth and Social Security Number, along with immigration information for non-citizens, against federal databases to confirm the employment eligibility of both citizen and non-citizen new hires. More than 80,000 U.S. businesses have automatically verified over 5.3 million workers so far, and on average, the program increases by about 1,000 new employers each week.

Protecting the Nation from Dangerous Goods

As a part of its risk-based approach, the department is focused on programs to identify, track, and intercept nuclear and radiological components and systems at ports of entry and in transportation systems within U.S. borders. The department is also intensifying efforts to strengthen capabilities that reduce the risk of a biological attack in the United States.

Comprehensive Radiation Detection: The Domestic Nuclear Detection Office (DNDO), in coordination with Customs and Border Protection (CBP) and the U.S. Coast Guard, has deployed more than 1,000 radiation detection devices to the nation's land and sea ports of entry. 100 percent of cargo containers crossing the southern border and 93 percent at the northern border are scanned for radiation, and more than 98 percent are scanned at our seaports. Three years ago, only 22 percent of incoming seaborne containerized cargo was being scanned for radiological and nuclear threats.

Ports, Waterways, and Coastal Security: Under Operation Neptune Shield, the U.S. Coast Guard escorts vessels carrying especially hazardous cargo, protecting them – and nearby population centers and infrastructure – from external attack. In 2007 alone, the Coast Guard escorted over 1,100 vessels/barges carrying such hazardous cargoes.

Record-Breaking Narcotics Seizures: The U.S. Coast Guard removed more than 355,000 pounds of cocaine at sea in fiscal 2007 – a record-breaking 160 metric tons – worth an estimated street value of more than $4.7 billion. CBP frontline personnel seized more than 3.2 million pounds of narcotics at and between ports of entry. In fiscal 2007 alone, ICE seized 241,967 pounds of cocaine, 4,331 pounds of heroin, 2,731 pounds of methamphetamine and 1.3 million pounds of marijuana. Additionally, ICE drug investigations led to 8,920 arrests and 5,539 convictions of individuals associated with narcotic violations.

Stemming the Flow of Weapons, Cash and Counterfeit Goods: ICE's Shield America program has achieved new successes in intercepting illegal exports of weapons, military equipment and sensitive technology, significantly increasing results with 188 arrests and 127 convictions in fiscal 2007. A new ICE initiative targeting unlicensed money services businesses that illegally transfer funds yielded 39 arrests, 30 convictions and seizures of more than $7.9 million.

Reducing Risk from Small Vessels: The U.S. Coast Guard has worked with small boat manufacturers, industry groups and the public to identify mitigation strategies to address the security risks posed by small vessels. The Coast Guard's 12 Maritime Safety and Security Teams, part of a 3,000 person Deployable Operations Group, are stationed at strategic ports nationwide and are uniquely trained to counter the small vessel threat. The Coast Guard and DNDO are collaborating with local authorities on a pilot program in Puget Sound and San Diego waterways on small vessel radiation detection.

BioWatch: Through aerosol collectors deployed by the Office of Health Affairs in over 30 jurisdictions across the nation, the BioWatch program provides critical early detection capability of dangerous biological pathogens. In the event of a widespread aerosolized anthrax attack, or other form of a weaponized biological agent, early detection and rapid distribution of life-saving medical countermeasures will be critical to saving countless lives. A next-generation BioWatch capability that could reduce detection time from up to 34 hours down to 4 to 6 hours is currently under development in partnership with the Science & Technology Directorate. Enhanced capabilities will continue to ensure rapid and reliable detection of the presence of dangerous biological agents.

Protecting Critical Infrastructure

The Department aims to protect critical infrastructure and key resources, essential government operations, public health and welfare, and the nation's economic and national security interests, working with private industry, which owns and operates roughly 85 percent of the nation's critical infrastructure.

Setting Chemical Security Standards: The National Protection and Programs Directorate (NPPD) established national standards for chemical facility security in a comprehensive set of regulations to protect chemical facilities from attack and prevent theft of chemicals that could be used as weapons.

Protecting Our Federal Networks: In January 2008, the President approved a new directive on cybersecurity policy. The President's classified directive establishes the policy, strategy and guidelines to secure federal systems. The directive provides a comprehensive approach that anticipates future cyber threats and technologies and requires the federal government to integrate many of its technical and organizational capabilities to better address sophisticated threats and vulnerabilities. DHS is leading many cybersecurity efforts under the Comprehensive National Cybersecurity Initiative, including the establishment and operation of a National Cyber Security Center (NCSC), a collaborative organization comprised of government agencies that will act like a hub for federal interagency information sharing. The mission of the NCSC is to detect, protect, analyze and distribute data related to threats on federal government networks.

Increasing Cyber Security: DHS has established the Computer Emergency Readiness Team (US-CERT) to provide a 24-hour watch, warning, and response operations center, which in 2007 issued over 200 actionable alerts on cyber security vulnerabilities or incidents. US-CERT developed the EINSTEIN intrusion detection program, which collects, analyzes, and shares computer security information across the federal civilian government. EINSTEIN is currently deployed at 15 federal agencies, including DHS, and plans are in place to expand the program to all federal departments and agencies. In addition, the Secret Service currently maintains 24 Electronic Crimes Task Forces to prevent, detect, mitigate and aggressively investigate cyber attacks on our nation's financial and critical infrastructures.

Greater Information Sharing: The Office of Intelligence and Analysis (I&A) leads DHS efforts to improve the sharing of information and intelligence with federal, state, local and tribal partners, and to change the departmental culture from a "need to know" approach to a "responsibility to provide." I&A has deployed 25 intelligence officers, as well as supporting information sharing systems, to fusion centers across the country.

Credentialing Port Workers: Since its October 2007 launch, more than 454,000 port workers have enrolled in the Transportation Worker Identification Credential (TWIC) biometric credential program, and thousands more are processed each week. More than 1.2 million longshoremen, truck drivers, port employees and others requiring unescorted access to secure areas of ports will be required to obtain a TWIC on a phased-in basis by April 15, 2009 and use it for port access.

Protecting the Federal Workforce: ICE's Federal Protective Service (FPS) officers protect approximately 9,000 federal facilities nationwide. In fiscal 2007, FPS was responsible for approximately 3,000 citations and arrests and intercepted roughly 760,000 prohibited items.

Counter-Improvised Explosive Device (IED) Efforts: In addition to TSA explosives detection technology at airports and

Transportation Security Officer training, science and technology development, and the coordination efforts of the Office for Bombing Prevention, the department has also made billions of dollars in grants available to states and communities for IED prevention and protection.

Addressing Biological Threats: The Office of Health Affairs has overseen the development and operational capabilities of the National Biosurveillance Integration Center (NBIC), which integrates biosurveillance data and information on biological incidents to enhance situational awareness. To date, NBIC has played an integral role in a number of recent biological events, including the recent Salmonella saintpaul outbreak, Foot-and-Mouth Disease, cases of Extremely Drug-Resistant Tuberculosis, as well as pet food and E. coli incidents. NBIC continues to enhance partnerships and coordination with federal agencies, state and local governments and the private sector through increased communications and development of daily situational reports and a biosurveillance common operating picture.

Building a Nimble, Effective Emergency Response System and a Culture of Preparedness

The Department continues to improve its capabilities and prepare those who respond to acts of terror and other emergencies by incorporating lessons learned from Hurricane Katrina, other disasters, and the 9-11 Commission Recommendations.

Response to over 400 Disasters: Since March of 2003, FEMA has responded to 454 major disaster and emergency declarations that included floods, tornadoes, winter and tropical storms, landslides and mudslides, earthquakes, droughts, typhoons and hurricanes. FEMA has provided direct material and financial assistance to more than 4 million individuals across the nation.

Federal Grant Programs: FEMA has provided extensive support to state and local governments to help them prepare for and mitigate the impact of natural and man-made disasters. Over the past five years, FEMA and DHS have provided over $23.8 billion for state and local projects through disaster grant programs, and an additional $2.5 billion in firefighter grants. With more than $26 billion provided to state and local partners and involving non-profit and private sector elements, FEMA has helped provide grants to improve our nation's preparedness for any disaster.

Sector Partnership Framework: The National Infrastructure Protection Plan (NIPP) was issued in 2006, and 17 Critical Infrastructure and Key Resources (CIKR) Sector Specific Plans were issued in 2007. In September 2008, an 18th sector – critical manufacturing – was recognized. The NIPP serves as the national plan to unify and enhance CIKR protection efforts through an unprecedented partnership involving the private sector, as well as federal, state, local and tribal governments. It sets forth a comprehensive risk management framework and clearly defined roles and responsibilities for all security partners.

Disaster Readiness and Support Activities: FEMA's expanded disaster operations and logistics management capabilities – including the creation of 214 pre-scripted mission assignments across 27 federal agencies that strengthen and streamline response capabilities, and the coordination of numerous nationwide exercises that include leaders at all levels of federal state and local government – have greatly improved our nation's ability to coordinate disaster response.

Supporting Local Security Plans: Protective Security Advisors work in state and local Emergency Operations Centers providing expertise and support to local authorities, the Principal Federal Official and the Federal Coordinating Officer responsible for domestic incident management, including the Virginia Tech shootings in Blacksburg, Va., the Chevron Refinery Fire in Pascagoula, Miss., the I-35W bridge collapse in Minneapolis, Minn., the Florida and California wildfires, and throughout the annual hurricane season.

Building Stronger Response Partnerships: DHS engaged state and local leadership, first responders and stakeholders on developing the National Response Framework, which outlines how our nation prepares for and responds to all-hazard disasters across all levels of government and community sectors.

Saved Over One Million Lives: The U.S. Coast Guard reached a remarkable milestone in 2007, saving more than 1,109,310 lives throughout its 217-year history.

Bolstering Emergency Communications: National Communication System's (NCS) National Coordinating Center for Communications (NCC) is the center of national security and emergency preparedness (NS/EP) communications during disasters. The NCC is a 24/7 operation and serves as the central coordination point between the Federal, State and local governments and the telecommunications industry during emergencies. The NCS runs the Telecommunications Service Priority (TSP) System to provide priority provisioning and restoration to telecommunications services during the preparation and recovery phases of an emergency. In addition, the NCS operates and maintains the Shared Resources High Frequency

Radio Network during an emergency event. The NCS also runs the Government Emergency Telecommunications Service and the Wireless Priority Service programs that provide federal, state and local leadership, first responders and leaders of critical infrastructure with priority call service in the event of network congestion on hard line and wireless networks.

Realizing Interoperable Communications: DHS, along with the Department of Commerce, has provided nearly $1 billion in Public Safety Interoperable Communications (PSIC) grants to help state and local first responders improve public safety communications and coordination during a natural or man-made disaster. In addition, the Science & Technology Directorate published results of the National Interoperability Baseline Survey – a nationwide survey of first responders and law enforcement that assesses progress in achieving interoperable communications. In addition, The Office of Emergency Communications (OEC) was established to serve as the departmental focal point for emergency communications. OEC completed the first-ever National Emergency Communications Plan this year, which provides a framework for emergency communications users across all levels of government.

Strengthening and Unifying DHS Operations and Management

DHS was created in 2003 to serve as the unifying core for the vast national network of organizations and institutions involved in securing our nation. DHS has further integrated core management functions and systems throughout headquarters and the components, achieving a more cohesive and unified department.

Consolidation of Network Sites: The department has consolidated more than 1,780 network sites into a single network that allows transparent monitoring of system performance and activity, prioritization of traffic, and a vastly improved security posture.

Improved Workforce Accommodations: The Office of the Chief Administrative Officer established initial DHS headquarters facilities, accommodated substantial growth, and set in motion a master building plan for consolidation of all headquarters functions. Planning includes the redevelopment of St. Elizabeths West Campus and reducing the number of locations within the National Capital Region from 40 locations to eight.

Enhanced Privacy, Civil Rights, and Civil Liberties: The Privacy Office and the Office for Civil Rights and Civil Liberties have worked to enhance privacy and civil rights and civil liberties through the department's work in cyber security, the use of satellite technology, airport screening protocols, and partnerships with Muslim-American communities.

Strengthened Business Processes and Technology: U.S. Citizenship and Immigration Services launched a new fee schedule designed to bring decades-old systems into the 21st century and improve customer service.

Enhancing Staffing and Training: In 2007, the Federal Law Enforcement Training Center trained a record 60,458 students from all three branches of the federal government, as well as international, state, local, campus, and tribal law enforcement agencies. In addition, DHS recently launched new training and communications tools including DHSCovery, a state-of-the-art online training system.

Improved Recruitment and Hiring: DHS decreased the average time it takes to hire new DHS employees, four days shorter than Office of Personnel Management targets. DHS also exceeded targeted goals by hiring more than 2,300 protection officers, 11,200 transportation security officers, over 700 immigration enforcement agents and over 450 deportation officers.

Intelligence Integration: The Under Secretary for I&A serves as the department's primary driver for integration of its intelligence equities and has taken significant steps to build and mature the DHS intelligence enterprise, including: to improve DHS' intelligence analysis, enterprise integration, and support to all its homeland security partners; establish the Homeland Security Intelligence Council, which comprises the heads of the intelligence components of the department; issue the DHS Intelligence Enterprise Strategic Plan that guides DHS Intelligence in furthering a strong, unified direction; and develop and implement appropriate directives, policies and procedures to uniformly lead, govern, integrate, and manage intelligence functions throughout DHS.

Building One DHS Acquisition Workforce and Streamlining Acquisitions: The Office of the Chief Procurement Officer is creating a unified DHS acquisition culture. Through the Acquisition Professional Career Program, the department is recruiting new talent for entry-level acquisition positions to develop a pipeline for future acquisition leaders. Acquisition process improvements ensured the critical U.S. Coast Guard Deepwater recapitalization program continued to move forward and resulted in the successful machinery trials of the first National Security Cutter, the USCGC BERTHOLF and the delivery of the first three *Ocean Sentry* Maritime Patrol Aircraft in 2007.

Systems Consolidation: The Office of the Chief Financial Officer is reducing the number of DHS financial systems to

realize cost savings and operational efficiencies. The department also will continue to consolidate its 17 legacy data centers into two enterprise-wide data centers. This consolidation will result in improved cyber security, information sharing and configuration management.

###

This page was last reviewed/modified on September 10, 2008.