Statement for the Record

Michael Chertoff
Secretary
United States Department of Homeland Security

Before the
United States Senate
Subcommittee on Homeland Security
Committee on Appropriations

April 20, 2005

Introduction

Mr. Chairman, Senator Byrd, and Members of the Subcommittee:

Thank you for the opportunity to address you today, and for your ongoing support of the Department of Homeland Security's efforts to keep America secure and free. I am honored and pleased to appear before the Senate Appropriations Committee, Subcommittee on Homeland Security. This is my first appearance before this Subcommittee, and I look forward to a productive exchange as the Department begins to reassess and readjust priorities and policies in accordance with the changing threat of terrorism over three and a half years after the September 11, 2001 attacks.

For more than two years now, the Department of Homeland Security has led a national effort to protect our country and our citizens from all manner of threats. It has been an honor to join the dedicated men and women who carry out this task daily. Ours is a difficult mission – to prevent another deadly and catastrophic terrorist attack such as the one we experienced on September 11, and if an attack occurs, to respond quickly and prevent further damage.

The 180,000-plus people of the Department carry out this mission with unflinching resolve and a driving determination that such an attack should never occur on American soil again. Realizing that we can make no guarantees, we pursue our mission with a sense of urgency and daily diligence, so that this nation can respond and recover quickly, should an incident or attack occur.

Since its establishment just over two years ago, DHS has made great strides in its efforts to unify the defense of our homeland. We have continued to integrate 22 distinct agencies and bureaus, each with its own employees, mission and culture.

But our security requires even greater coordination and effort throughout the Department, across all levels of government, and throughout our nation to create synergy and new capabilities. It requires an unwillingness to accept complacency as part of anything we do; rather, we know we must apply all effort to tear down stove-pipes and coordinate key intelligence, policy, and operational issues across DHS and the government.

Second Stage Review

I have therefore initiated a comprehensive review of the organization, operations and policies of the Department as a whole. This comprehensive review will examine what we are doing and what we need to do without regard to component structures and programmatic categories.

We want to understand better what's working and what isn't. We will be evaluating every element of our working mission and making sure that the Department is best organized to meet the threats – both current and future – that face our nation.

Old categories, old jurisdictions, old turf will not define our objectives or the measure of our achievements because bureaucratic structures and categories exist to serve our mission, not to drive it.

Deputy Secretary Michael Jackson has been charged with overseeing this process. The goal of the review is to help me make informed decisions as I lead the Department. Deputy Secretary Jackson has selected a team of Department officials to look at a number of critical cross-cutting issues and determine how departmental resources and programs can be most effectively applied to achieve our security goals. I have asked them to get back to me by Memorial Day with the bulk of their recommendations. I intend to study and act on their recommendations.

What will the review cover? Take an issue such as maritime cargo security, which cuts across several departmental components. Customs and Border Protection, Coast Guard, Science and Technology, and Information Analysis and Infrastructure Protection each address aspects of this overall mission. Each might perform its element well, but we must go further to ensure that each is performing seamlessly and in coordination with the others, that we eliminate any duplication of effort, and that we reap the full strength of our wide spectrum of capabilities.

Of course, in executing the initial phase of putting the Department together and integrating the different components into a working structure, my predecessor and the men and women of Homeland Security did a tremendous job. They should be commended.

Now, as we enter into the second phase of the Department's life, we must also take a fresh, creative look at the Department itself – including its organization, its operations, and its policies. We are not yet fully integrated and our entities are still not always coordinated with each other. Now the challenge is to take the advantage of two years' experience and evaluate the Department to see if there are potential structural and operational changes that will improve and enhance our capabilities to protect and safeguard this nation.

Cross-Cutting Functions and Integration

On the most basic level, we need to take a step back and focus on the fundamental question: Why was the Department of Homeland Security created? It was not created merely to bring together different agencies under a single tent. It was created to enable these agencies to secure the homeland through joint, coordinated action. Our challenge is to realize that goal to the greatest extent possible.

Let me tell you about three areas where I plan to focus our efforts to achieve that goal. First, we need to operate under a common picture of the threats that we are facing. Second, we need to respond actively to these threats with the appropriate policies. Third, we need to execute our various component operations in a unified manner so that when

we assess the intelligence and we have decided upon the proper policies, we can carry out our mission in a way that is coordinated across the board.

My intent is to integrate each of these three areas -- intelligence, policy, and operations -- across the Department, so that each is directed from the most senior level of the Department.

Let me turn to intelligence. Intelligence plays a pivotal role in mapping our mission. When the Department was created, 22 separate and distinct entities were woven together, a number of which had components focused on intelligence-gathering and analysis. One of my top priorities is to make sure that these various intelligence components function as a cohesive unit, and that our information and analysis is coordinated across the Department so that DHS, as a full member, can enhance its contribution to the Intelligence Community.

First, we must organize and combine all intelligence within DHS. To do this effectively, we must ensure that our own intelligence components are interoperable. The Department has already made progress in this area. For example, the Homeland Security Operations Center was stood up to help the Department develop a common operating picture and facilitate information sharing.

We must make sure that we are gathering all relevant information from the field, communicating with each other, and approaching analysis with a mission-oriented focus. We must ask, for example, whether those who evaluate the border from the Customs and Border Protection perspective are learning from analysts in the U.S. Coast Guard. They each look at border security, but from different vantage points. Only if they are working together can they fill in key gaps, paint a realistic picture, and evaluate all of the different pieces of information and intelligence that they are each gathering. We have to maximize the fact that all of these components now exist under the same umbrella.

Second, we must make sure that information is being disseminated both up and down the ranks of the Department. Strong and effective coordination does not just mean that our analysts at DHS headquarters are working together. We need to fuse and exploit all the information that we learn across the country, so that when a Border Patrol agent in Texas learns of a new alien smuggling method, that information is fed up to our intelligence analysts, incorporated where appropriate into our strategy to combat smuggling, and disseminated across the Department to others focused on the same problem. We must build a culture in which the disparate pieces of information are being transmitted to our analysts so that they, who have the benefit of the fuller picture, can properly analyze all of our information and inform our decision-making.

The converse must be true when our intelligence analysts learn of new vulnerabilities that terrorists are trying to exploit. That same agent in Texas needs to know, on a timely basis, of the threat and what he should be looking out for. We have a great many talented individuals at the Department. Some gather and analyze intelligence. Others learn critical information as they are in the field performing their jobs. The opportunities are

endless. DHS needs to bring all of these nuggets of information together and disseminate them appropriately. We need to have the structure and the correct systems and technologies in place to take full advantage of them.

Third, our focus must extend beyond the Department itself. We must review and make use of intelligence coming from the Intelligence Community and we must play an active role in providing intelligence information to the Intelligence Community. As the WMD Commission made clear in its report two weeks ago, sharing information across the Federal Government is critical if we are to succeed. To that end, I am committed to making sure that our law enforcement and intelligence partners across the Federal Government have appropriate access to the Department's information and analysis, to the maximum extent possible under the law, while protecting the privacy rights and civil liberties of Americans. By the same token, we must sit as full partners at the table with full access to others in the Intelligence Community. We must work in concert with the Intelligence Community. I will work closely with the Director of National Intelligence, whose job it will be to make sure that the Intelligence Community is well-coordinated and mission-focused.

In addition, intelligence and information from other Federal agencies is critical to our efforts to secure the homeland. The development of the terrorism information sharing environment, as called for under the Intelligence Reform and Terrorism Prevention Act, will connect the resources (people, systems, databases, and information) of Federal, State, and local governments, and the private sector allowing users to share information and improve collaboration.

Finally, we must inform and communicate with our State, local, tribal entities, and private sector partners. As I observed just last week during TOPOFF, when it comes to securing the nation, we must ensure that these entities are well-equipped both to react to crisis and to prevent it. As part of this effort, we must improve our ability to operationalize intelligence. As information comes in, we need to make sure it is getting out to the right people and in a way that they can use to strengthen their efforts and contribute effectively to ours. Intelligence in a vacuum is meaningless. We need to explain how our outside partners can counter that threat and what we need them to do to watch out for it.

Now, let me address policy development. Development and coordination of policy are major responsibilities of this Department. The Department has the central mission of securing the homeland, but there are many different aspects of that mission with numerous contributors. Large elements of DHS include traditional operational functions in which we deploy personnel, equipment, planes, ships and vehicles. But other elements principally involve planning and rule making, and networking with State, local, and tribal entities, and private parties. All of these must serve and promote our homeland security imperatives.

Therefore, we need to further enhance our capability to think through broad and over-arching issues like border security, emergency preparedness, transportation security, and

cargo security, with a Department-wide perspective, rather than just through the lenses of one particular component. We need to develop our policies by first looking at our missions and asking the comprehensive, result-oriented questions, rather than by looking to one particular entity that has the lead in driving an issue to conclusion.

Accordingly, I believe that we should pull together the vast expertise and the varying perspectives already at the Department as we work toward integrating our many cross-cutting functions. For this reason, one of the areas that we are closely studying in the Second Stage Review is the advisability of creating a department-wide, substantial policy office. This office will also be a very important focal point for coordinating DHS's policy work with other Federal, State, local, and tribal entities.

Finally, let me discuss operational coordination. Just as with intelligence and policy, we need to find new ways to increase our operational coordination. Diverse operational components were woven together when Congress stood up the Department, each with its own history and identity. As I have become acquainted with these various components, I have quickly learned that there is a great deal of talent within them. Each entity has its own unique focus, but often they address the same mission from differing perspectives. But we cannot function as a cohesive unit, unless each operational component works together in combination to promote common missions.

This means that our operations must be driven by mission-oriented plans. It can no longer be the case that different components tackle different problems each in its own way and then later look to see if the pieces fit together. Whether it is preventing a potential act of terrorism, emergency preparedness, border protection, or countering a particular threat, we must first define the mission and second deploy all the tools within the Department to effectively execute each operation.

The Department has already begun this process. To take but one example, on the Arizona border, we have a cross-cutting initiative to protect the border, integrating intelligence gathering, border enforcement, and monitoring. It encompasses the efforts of several of our agencies, including Customs and Border Protection, Immigration and Customs Enforcement, Science and Technology, the Coast Guard, and Information Analysis and Infrastructure Protection. Each plays an integral role. The operations themselves involve patrolling the border, generating information, and using it to take enforcement actions. The genius of the Department of Homeland Security is that we have the capability within one department to do all of these things. But we need to carry out joint operational activities and have a joint perspective on a routine basis, not only when we stand up a special project.

Operations are also the mechanisms by which we respond to crisis. We cannot wait for a crisis, however, to learn, for example, whether TSA has the capability to communicate effectively and coordinate with FEMA. Nor can we learn in crisis that both are conducting the same operations or sending different messages to the private sector. The Department has made significant progress in this area. For example, it developed the National Response Plan to more effectively map out how to handle crisis situations. Now

is the time to organize around missions rather than old bureaucracies, work through all of these potential disconnects in our systems, and operate as one unified Department. But integrating ourselves cohesively is not enough.

Risk-Based Approach

I have been saying, and you will continue to hear me say, that we need to adopt a risk-based approach in both our operations and our philosophy. America is dynamic. Our strength as Americans is the sum of every generation that has ever been born in or immigrated to this great land. Our wealth and livelihoods are advanced by the inspired ideas and innovation of our own people. We prosper through the vast opportunities that exist to interact with the global economic community.

Risk management is fundamental to managing the threat, while retaining our quality of life and living in freedom. Risk management must guide our decision-making as we examine how we can best organize to prevent, respond and recover from an attack. We need to be realistic in our prioritization. We must assess the full spectrum of threats and vulnerabilities.

We all live with a certain amount of risk. That means that we tolerate that something bad can happen; we adjust our lives based on probability; and we take reasonable precautions. So, too, we must manage risk at the homeland security level. That means developing plans and allocating resources in a way that balances security and freedom when calculating risks and implementing protections.

The most effective way, I believe, to apply this risk-based approach is by using the trio of threat, vulnerability, and consequence as a general model for assessing risk and deciding on the protective measures we undertake.

Here I inject a note of caution because the media and the public often focus principally on threats. Threats are important, but they should not be automatic instigators of action. A terrorist attack on the two-lane bridge down the street from my house is bad but has a relatively low consequence compared, to an attack on a major metropolitan multi-lane bridge. At the other end of the spectrum, even a remote threat to detonate a nuclear bomb is a high-level priority because of the catastrophic effect.

Each threat must be weighed, therefore, along with consequence and vulnerabilities. As consequence increases, we respond according to the nature and credibility of the threat and any existing state of vulnerabilities. Our strategy is, in essence, to manage risk in terms of these three variables – threat, vulnerability, consequence. We seek to prioritize according to these variables…to fashion a series of preventive and protective steps that increase security at multiple levels. We must examine the mission and work of all elements of DHS through this template of consequence, vulnerability and threat. Have we fully defined our missions? How far have we gone in carrying them out? What more needs to be done?

The Department is already working with State, local, and private sector partners to further refine the Interim National Preparedness Goal to aid the targeting of resources to where the risk is greatest. There is much that we are doing. DHS agencies, for example, have provided unprecedented level of funding and resources since 9/11 to State, local and private sector partners to protect and prepare America's communities and individual citizens. We continue to improve the ways for first responders across the nation to be better equipped, better trained and more capable of communicating across the public safety community. But we must bring even greater focus and discipline to our preparedness mission. We need to take a very substantive look at how we align our preparedness activities and functions. We need to look at how best to configure our organizations, operations, programs and policies so that we can think strategically about preparedness.

What should drive our intelligence, policies, operations, and preparedness plans and the way we are organized is the strategic matrix of threat, vulnerability and consequence. And so, we'll be looking at everything through that prism and adjusting structure, operations and policies to execute this strategy.

FY 2005 Accomplishments

Before beginning to outline the major themes of the Department's FY 2006 Budget request, I would like to highlight a few of the Department's accomplishments over the past year, including the following:

- The Department established "the One-Stop-Shop" for first responder grants which allows a single point of entry to the federal government for homeland security preparedness resources.
- DHS has provided unprecedented levels of funding and resources to state, local and private sector partners to protect and prepare America's communities and individual citizens. We continue to improve ways for first responders across the nation to be better equipped, better trained and more capable of communicating across the public safety community.
- U.S. Citizenship & Immigration Services (USCIS) is on track to eliminate the backlog of immigration benefit applications by the end of FY 2006. In FY 2004, the agency increased productivity by 21 percent and successfully reduced the backlog to 1.3 million cases – down from a high of 3.8 million cases in January 2004.
- United States-Visitor and Immigrant Status Indicator Technology (US-VISIT) was successfully implemented at 115 U.S. international airports and 14 seaports and immediately demonstrated results by preventing individuals with criminal records and immigration violations from entering the U.S. In addition, US-VISIT successfully deployed initial capability to the 50 busiest land border ports of entry in December 2004 and was also deployed at pre-clearance airports in Canada, Bermuda, the Caribbean and Guam.

- The U.S. Coast Guard (USCG) developed, reviewed, and approved 9,000 domestic vessel security plans; 3,200 domestic facility plans; 48 Area Maritime Security Plans and Committees; and verified security plan implementation on 8,100 foreign vessels.
- USCG interdicted nearly 11,000 undocumented migrants attempting to enter the country illegally by sea, saved the lives of nearly 5,500 mariners in distress and responded to more than 32,000 calls for rescue assistance.
- Counterdrug efforts remain a top priority for the Department. With the passage of the December 2004 Intelligence and Reform Bill, the Department's Office of Counternarcotics Enforcement is heavily invested in ensuring counterdrug operations and policy are synchronized across the Department, and that our components are adequately resourced to perform their counterdrug mission. In FY 2004, the Coast Guard, Immigration and Customs Enforcement, and Customs and Border Protection collectively kept 489,870 pounds of cocaine from reaching the streets of our nation.
- In support of Operation Iraqi Freedom the USCG protected, safely secured, and escorted to sea over 200 military sealift departures at ten different major U.S. seaports, carrying over 25 million square feet of indispensable cargo.
- The Homeland Security Operations Center (HSOC) Homeland Security Information Network (HSIN) infrastructure to facilitate providing Secret level connectivity has been expanded to state level Emergency Operations Centers in all 50 states, territories, and the District of Columbia.
- The Department's Information Sharing and Collaboration Office (ISCO) is responsible for producing immediate, near-term and long-term improved information sharing processes and systems. ISCO successfully partnered with DoJ to establish a first ever capability to share information between systems supporting law enforcement users across the country. The Homeland Security Information Network (HSIN), Regional Information Sharing System (RISS), Law Enforcement On-line (LEO), and Criminal Information Sharing Alliance Network (CISANet) now share information posted on each system with the users of the other systems with the result that over 7,000 documents are already posted and the numbers are growing every day. Users are able to access information on any of the four systems through a single sign-on, thus eliminating the need to access all four network simultaneously.
- Working closely with importers, carriers, brokers, freight forwarders and others, Customs and Border Protection (CBP) has developed the Customs-Trade Partnership Against Terrorism (C-TPAT) program, which has become the largest government/private partnership to arise from September 11th.
- In carrying out its agricultural mission, Customs and Border Protection (CBP) Agricultural Specialist conducted 3,559,403 cargo inspections, 111,416,656 passenger inspections and made more than 400,000 interceptions of prohibited meat and animal by-products. During the same time period, CBP agricultural

specialists intercepted more than 96,000 prohibited plant materials and found more than 64,000 agricultural pests.

- The Federal Emergency Management Agency (FEMA) provided $4.9 billion in aid, including hurricane relief efforts for victims and communities affected by disasters. FEMA, with its DHS counterparts, responded to 65 major disaster declarations and seven emergencies in FY 2004.
- Passenger screening by the Transportation Security Administration (TSA) kept 6,501,193 prohibited items from coming on board aircraft during FY 2004.
- In 2004, TSA screened approximately 600 million checked bags using advanced explosive detection technologies and over 31 million mail parcels using explosive detection canine teams.
- Since establishment of the Federal Flight Deck Officer (FFDO) Program in February 2003, TSA has selected, trained, and armed thousands of volunteer flight crewmembers to defend the flight decks of commercial passenger and cargo aircraft against acts of criminal violence or air piracy. To date, hundreds of thousands of flights have been protected by one or more FFDOs serving in mission status.
- A total of 428 million people, including 262 million aliens, were processed at land, air and sea ports of entry. Of that number 643,000 aliens were deemed inadmissible under U.S. law.
- Immigration and Customs Enforcement (ICE) officers achieved a 112 percent increase over the prior year for fugitive apprehensions resulting in more than 7,200 arrests. ICE removed more than 150,000 aliens in 2004.
- Border Patrol agents apprehended almost 1.2 million illegal aliens between our official ports of entry.
- The Container Security Initiative (CSI), which involves pre-screening shipping containers to detect and interdict terrorists' weapons and other illegal material, was expanded to include 21 countries. CSI is now operational in 34 foreign ports in Europe, Asia, and Africa.
- Approximately 600 million checked bags were screened using advanced explosive technologies in 2004.
- More than 2,500 criminal investigations were conducted involving the illegal export of U.S. arms and strategic technology, including Weapons of Mass Destruction (WMD).
- The Federal Law Enforcement Training Center (FLETC) provided basic and advanced law enforcement training to more than 44,750 students, representing 81 federal agencies, as well as state, local and international law enforcement organizations.

- Border and Transportation Security (BTS) assumed responsibility for visa policy under the Homeland Security Act and implemented improvements in visa review times and transparency.
- The Department planned, designed, and implemented security for five events designated as *National Security Special Events* (State of Union Address, G-8 Economic Summit, Former President Ronald Reagan Funeral, Democratic National Convention and Republican National Convention) as well as the support, integration, and coordination of hundreds of national special events not meeting the National Security Special Events designation.
- USSS arrested 30 individuals involved in global cyber organized crime, domestically and internationally. Industry experts estimate that $1 billion in total fraud loss was prevented.
- The Science and Technology (S&T) Directorate has implemented initiatives in chemical, biological, radiological, nuclear, and explosive (CBRNE) countermeasures, cargo security, border and transportation security, interoperability, standards for emergency responders, and cyber security. These initiatives have resulted in improved security of U.S. borders, transportation systems and critical infrastructure, and resulted in the greater preparedness of our nation. To date, Department officials have visited more than 200 chemical, petrochemical, water, energy, (i.e. electricity, oil, liquefied natural gas, pipelines, storage, etc.) agriculture, commercial assets, national icons, soft targets, and mass transportation centers.
- The Department established the National Cyber Response Coordination Group (NCRCG) in partnership with the Department of Justice and the Department of Defense, as a forum of 13 principal agencies that coordinate intra-governmental and public/private preparedness operations to respond to and recover from large-scale cyber attacks.
- The Department co-sponsored Blue Cascades II and Purple Crescent II, two regional tabletop cyber exercises in Seattle, WA and New Orleans, LA. Each exercise brought together more than 200 government and private sector officials to examine cyber security readiness and response procedures, highlight the importance of cyber security in critical infrastructure protection, and discuss solutions for integrating physical security and cyber security. Region-specific coordination and communication plans between first responders, the federal government, and critical infrastructure owners/operators were exercised.
- The Department established the US-CERT Control Systems Center to bring together government, industry, and academia to reduce vulnerabilities, respond to threats, and foster public/private collaboration to improve the security of the data and process control systems that operate our nation's critical infrastructures.
- The Department established the Control Systems Security and Test Center (CSSTC) in conjunction with Idaho National Environmental and Engineering Laboratory, to provide an opportunity for government and industry to collaborate

on cyber vulnerability enumeration and reduction activities for control systems currently in use across critical infrastructure sectors. The CSSTC models map the cause and effect relationships of cyber attacks on control systems, assess the outcomes of actual events in a simulated environment, and provide the US-CERT with response and mitigation actions to share with partners in the control systems community.

- DHS and the Germany Ministry of the Interior jointly hosted a Multilateral Cyber Security Conference in Berlin, Germany. The conference brought together cyber security policymakers, managers from computer security incident response teams with national responsibility, and law enforcement representatives responsible for cyber crime from 15 countries. The conference program included a facilitated tabletop exercise and interactive discussions on how to develop an international framework – as well as near term actionable steps – for watch, warning, and incident response.

- The Information Analysis and Infrastructure Protection (IAIP) Directorate has developed and disseminated warning products (i.e. warning messages) to federal, State, territorial, tribal, local, private sector, and international partners to protect citizens, governments, critical infrastructure, and key assets.

- IAIP has produced more than 70 "Common Vulnerability" reports executed over 250 Site Assistance Visits, nearly 600 Buffer Zone Protection Plans, and is continuing to build the National Asset Database. As of today, more than 80,000 "assets" have been compiled.

- Uninterrupted communications are critical for national security and emergency preparedness personnel in responding to a crisis. The National Communications System (NCS) issued an additional 17,000 calling cards, further enabling priority wire line phone communications and an additional 8,000 cell phones for priority wireless communications. In past disasters and crises, these capabilities have proved crucial.

- Pursuant to Homeland Security Presidential Directive – 7, IAIP is coordinating the overall national effort to enhance the protection of the critical infrastructure and key resources of the United States and has distributed the Interim National Infrastructure Protection Plan (Interim NIPP) to other Federal departments and agencies, the State Homeland Security Advisors, and the private sector stakeholder groups (e.g., the Homeland Security Advisory Council, Sector Coordinating Council, ISAC Councils, National Infrastructure Advisory Council, the U.S. Chamber of Commerce, etc.) The Interim NIPP provides a risk management framework for integrating and coordinating the Nation's infrastructure protection activities that takes into account threats, vulnerabilities, and consequences to manage a broad range of risks across the Nation's 17 critical infrastructure sectors.

- These important DHS activities were analyzed where appropriate for their impacts on personal privacy and civil liberties.

FY 2006 Budget Request

The Department's FY 2006 Budget request revolves around five major themes: Revolutionizing the Borders; Strengthening Law Enforcement; Improving National Preparedness and Response; Leveraging Technology; and Creating a 21st Century Department.

I. Revolutionizing the Borders

September 11, 2001 demonstrated the sobering reality that the U.S. is no longer immune from catastrophic attack. No longer do vast oceans and friendly neighbors provide the buffer against aggressive adversaries. In order to maximize the security of our nation against persons determined to undermine the economy of the U.S., our way of life and the freedoms we enjoy, the Department is determined to deter, thwart, and remove any threat to the nation long before it reaches our borders. During FY 2005, we will continue to strengthen our border security. For FY 2006, the President's Budget includes several initiatives aimed at revolutionizing the Borders.

Weapons of Mass Destruction (WMD) Detection Technology is an integral part of the Domestic Nuclear Detection Office (DNDO) that includes a comprehensive strategy to address the threat of nuclear and radiological terrorism. The Budget includes $125 million to purchase additional Radiation Portal Monitors (RPMs) and pilot advanced next generation RPMs to detect both gamma and neutron radiation at our borders. In addition, the Container Security Initiative (CSI), which focuses on pre-screening cargo before it reaches our shores, will have a preventative and deterrent effect on the use of global containerized shipping of WMD and other terrorist equipment. Egypt, Chile, India, the Philippines, Venezuela, the Bahamas and Honduras have been identified as expansion locations for this initiative in FY 2006. An increase of $5.4 million over FY 2005 is included in Customs and Border Protection (CBP) budget for CSI. The total amount in the President's Budget for CSI is $138.8 million.

CBP's America's Shield Initiative (ASI) enhances electronic surveillance capabilities along the Northern and Southern land borders of the U.S. by improving the sensor and video surveillance equipment deployed to guard against the entry of illegal aliens, terrorists, WMDs and contraband into the U.S. The Budget includes $51.1 million for ASI, an increase of $19.8 million. With additional technology investments, the President's Budget proposes to increase Border Patrol staffing over current levels to backfill staff vacated along the Southwest border, as well as increase staffing levels assigned to coastal areas. Since September 11, 2001, some Border Patrol agents were shifted to the Northern border in order to increase the number of agents assigned there. An increase of 210 positions and $36.9 million is included in the Budget for the Border Patrol. This increases the number of Border Patrol Agents to 10,949.

The Customs Trade Partnership Against Terrorism (C-TPAT), which began in November 2001, is another essential cargo security effort. C-TPAT focuses on partnerships along the entire supply chain, from the factory floor to foreign vendors to land borders and seaports. The President's Budget includes an increase of $8.2 million for this effort, bringing total funding for C-TPAT to $54.3 million. These funds will be used to enhance our ability to conduct additional supply chain security validations.

In addition to enhancing secure trade programs, the President's Budget also seeks to support additional investments in CBP's National Targeting System. CBP Targeting Systems aid in identifying high-risk cargo and passengers. The Budget includes a total of $28.3 million for these system initiatives, of which $5.4 million is an increase over the FY 2005 level. Further**,** US-VISIT, which will be consolidated within the Screening Coordination Office, will increase from $340 million to $390 million in the Budget. The increase will provide for the accelerated deployment of US-VISIT at the land border and enhanced access for border personnel to immigration, criminal and terrorist information.

The President's 2006 Budget includes $966 million for the Integrated Deepwater System (IDS) to help address the Coast Guard's declining readiness trends and to transform the Coast Guard with enhanced capabilities to meet current and future mandates through system-wide recapitalization and modernization of Coast Guard cutters, aircraft, and associated sub-systems. Among other things, the IDS request funds production of the third Maritime Security Cutter-Large and continues HH-65 helicopter re-engineering to eliminate safety and reliability issues in the Coast Guard's operational fleet of short range helicopters.

Finally, within CBP, Long Range Radar technology is used by the Office of Air and Marine Operations to detect and intercept aircraft attempting to avoid detection while entering the U.S. CBP and the Department of Defense will assume responsibility for operating and maintaining these systems from the Federal Aviation Administration (FAA) beginning in FY 2006. CBP's share is $44.2 million in the Budget.

II. Strengthening Law Enforcement

Law enforcement is a critical element in preventing terrorism across the nation. Whether at the federal, state, or local level, law enforcement agencies perform this vigilant task. As we know from unfortunate first hand experience, the known threats are creative, clever, and sophisticated. The Department's law enforcement agencies need to stay ahead of the threat. To achieve this, the Budget includes funding for numerous key initiatives to maintain and strengthen current law enforcement initiatives both within and beyond our borders.

The United States Coast Guard (USCG) is the nation's leading maritime law enforcement agency. The President's Budget seeks additional investment in USCG assets to enhance its ability to carry out its mission. The President's budget provides $11 million to increase port presence and Liquefied Petroleum Natural Gas (LNG) transport security, funding additional Response Boat-Smalls and associated crews to increase presence for

patrolling critical infrastructure, enforce security zones, and perform high interest vessel escorts in strategic ports throughout the nation. This initiative also provides additional boat crews and screening personnel at key LNG hubs such as Baltimore, MD and Providence, RI to enhance LNG tanker and waterside security.

In addition, in the President's Budget, the Armed Helicopter for Homeland Security Project increases by $17.4 million. These funds will provide equipment and aircraft modifications to establish armed helicopter capability at five USCG Air Stations. This will provide the USCG and DHS with the tools needed to respond quickly and forcefully to emergency maritime threats. A total of $19.9 million is included in the Budget for this project. Finally, the Response Boat-Medium Project increases by $10 million the effort to replace the USCG's 41-foot utility boats and other large non-standard boats with assets more capable of meeting all of the USCG's multi-mission operational requirements. A total of $22 million is proposed in the Budget for this effort.

U.S. Immigration and Customs Enforcement (ICE), the largest investigative arm of the Department of Homeland Security (DHS), is responsible for identifying and shutting down vulnerabilities in the nation's border, economic, transportation and infrastructure security. The President's Budget seeks a 13.5 percent budget increase for ICE, including increasing the Detention and Removal program by $176 million. For the Temporary Worker program, the Budget seeks to more than double the resources available for worksite enforcement including employer audits, investigations of possible violations and criminal case presentations. An increase of $18 million is proposed in the Budget for this effort. The President's Budget seeks a total of $688.9 million for ICE's Federal Air Marshal Service. This funding will allow ICE to protect air security and promote public confidence in our nation's civil aviation system.

The Department's FY 2006 Budget includes several other funding enhancements for law enforcement, including:

- The Federal Law Enforcement Training Center's (FLETC) budget increases by $2.7 million for Simulator Training Technology to teach officers and agents how to avoid collisions and reduce the dangers associated with pursuit driving.

- Federal Flight Deck Officers (FFDO)/Crew Member Self-Defense (CMSD) Training is increased by $11 million in FY 2006. This allows for the expansion of the semi-annual firearm re-qualification program for FFDO personnel and to fund the first full year of the CMSD training program. A total of $36.3 million is included for FFDO/CMSD in the Budget.
- Enhancing law enforcement training through co-location of the Coast Guard's Maritime Law Enforcement Training program with the Federal Law Enforcement Training Center, increasing maritime law enforcement training throughput and promoting better coordination among field activities with other Federal, state, and local agencies.

III. Improving National Preparedness and Response

Though the primary mission is to protect the nation from terrorism, the Department's responsibilities are diverse. No DHS effort has a greater scope, reach and impact upon the citizens across the U.S. than our efforts to prepare the nation to respond to major acts of terror or natural disaster. This Budget continues to support the President's homeland security directives that establish the methods and means by which our nation prepares for and responds to critical incidents. Since its establishment, the Department has, and continues to provide, an unprecedented level of financial support to the state, local, and tribal governments and to certain private sector entities. The Budget builds on these efforts and proposes significant resources to provide direct financial assistance to our nation's first responders, emergency managers, and citizen volunteers. There are several initiatives in the Budget geared towards improving national preparedness and response.

The FY 2006 budget continues to support the nation's first responders and seeks a total of $3.6 billion to support first-responder terrorism preparedness grants, administered by the Office of State and Local Government Coordination and Preparedness, with better targeting to high-threat areas facing the greatest risk and vulnerability. This funding will support state and local agencies as they equip, train, exercise, and assess preparedness for major emergencies, especially acts of terrorism. While there may be gaps in state and local capabilities, we believe special emphasis must be given to communications interoperability, catastrophic planning, WMD awareness, critical infrastructure protection, and cross-jurisdictional/regional cooperation and interaction.

For FY 2006, the President's Budget proposes $20 million for the Federal Emergency Management Agency's (FEMA) enhanced catastrophic disaster planning. This funding will support catastrophic incident response and recovery planning and exercises. FEMA will work with states and localities, as well as other federal agencies to develop and implement plans that will improve the ability of federal, state, or local governments to respond to and to recover from catastrophic disasters quickly and effectively. FEMA will address the unique challenges a catastrophic disaster situation poses, including food and shelter, transportation, decontamination and long term housing needs.

On October 1, 2004, the Department of Homeland Security launched the Office of Interoperability and Compatibility designed to help state and local public safety practitioners improve communications interoperability. The Office of Interoperability and Compatibility (OIC), part of the Science & Technology directorate, oversees the wide range of public safety interoperability programs and efforts currently spread across Homeland Security. These programs address critical interoperability issues relating to public safety and emergency response, including communications, equipment, training, and other areas as needs are identified. The OIC allows the Department to expand its leadership role in interoperable communications that could be used by every first responder agency in the country. The OIC has currently identified three program areas: Communications, Equipment, and Training. With $20.5 million in FY 2006, the OIC will plan and begin to establish the training and equipment programs, as well as continue existing communication interoperability efforts through the SAFECOM Program.

The President's FY 2006 Budget for the Department proposes other enhancements to improve our national preparedness and response, including:

- Replacement of the USCG's High Frequency (HF) Communications System. Funded at $10 million in the Budget, this system will replace unserviceable, shore-side, high power high frequency transmitters, significantly improving long-range maritime safety and security communications.

- The Budget increases Cyber Security to enhance the U.S. Computer Emergency Preparedness Team (US CERT), a 24/7 cyber threat watch, warning, and response capability that would identify emerging threats and vulnerabilities and coordinate responses to major cyber security incidents. An increase of $5 million is proposed, bringing the program total to $73.3 million.

- The Rescue 21 project is funded at $101 million in the Budget to continue recapitalizing the Coast Guard's coastal zone communications network. This funding will complete system infrastructure and network installations in 11 regions and begin development of regional designs for the remaining 14 regions.

IV. Leveraging Technology

Rapid advances in technological capability are allowing the Department personnel to protect the homeland more efficiently and effectively across many components. To prepare the nation to counter any WMD threat—threats from CBRNE substances—this Budget includes an increase for new initiatives that support research and development to counter these weapons and their potentially devastating effects.

First, the Domestic Nuclear Detection Office (DNDO) is being established as a joint national office to protect the nation from radiological and nuclear threats. This office will consolidate functions within DHS and establish strong interagency linkages for the deployment of a national domestic nuclear detection architecture, the conduct of transformational research and development (R&D), and the establishment of protocols and training for the end users of equipment developed and deployed through the new office. The DNDO will integrate domestic nuclear detection efforts undertaken by individual federal agencies, state and local governments, and the private sector and be closely linked with international nuclear detection efforts. A total of $227.3 million is requested for this effort in FY 2006.

Second, TSA's emerging checkpoint technology is enhanced by $43.7 million in FY 2006 to direct additional resources to improve checkpoint explosives screening. This request responds to the 9/11 Commission Report's finding that investments in technology may be the most powerful way to improve screening effectiveness and priority should be given to explosive detection at airport checkpoints for higher risk passengers immediately. This new equipment assures that TSA is on the cutting edge, ahead of the development of increasingly well-disguised prohibited items. This proposed increase

will result in investing more than $100 million in FY 2005 and FY 2006 for new technology to ensure improved screening of all higher risk passengers.

In addition, to improve TSA's information technology network, the President's Budget includes $174 million to complete installation of High Speed Operational Connectivity (Hi-SOC) to passenger and baggage screening checkpoints to improve management of screening system performance. Within the Screening and Coordination Office, funding is sought for the Secure Flight and Crew Vetting programs -- an increase of $49 million to field the system developed and tested in FY 2005. The funds will support testing information systems, connectivity to airlines and screen systems and daily operations. This also includes an increase of $3.3 million for crew vetting.

Third, the President's Budget also proposes additional funding for two critical Department programs – the Homeland Secure Data Network (HSDN) and the Homeland Security Operations Center (HSOC). For FY 2006, the Budget includes $37 million for HSDN. This funding will streamline and modernize the classified data capabilities in order to facilitate high quality and high value classified data communication and collaboration. Funding for the HSOC is increased by $26.3 million, bringing its FY 2006 funded level to $61.1 million. This includes an increase of $13.4 million for the Homeland Security Information Network (HSIN) and an increase of $12.9 million to enhance HSOC systems and operations. The funding will provide the HSOC with critical tools for sharing both classified and unclassified information and situational awareness with federal, state, local and tribal governments.

Fourth, a key element of the Department's Maritime Security Strategy is to enhance Maritime Domain Awareness (MDA), leveraging technology to improve sharing of accurate information, intelligence, and knowledge of vessels, cargo, crews and passengers, mitigating threats to the security, safety, economy, or environment of the U.S.. The FY 2006 budget funds several key MDA initiatives, including $29.1 million for the nationwide Automatic Identification System (AIS) and $16.5 million to provide additional maritime patrol aircraft flight hours in support of detection, surveillance and tracking activities.

Finally, the Department is seeking additional technology investments in other critical areas, such as:

- $20 million for developing a Low Volatility Agent Warning. This system will serve as the basis for a warning and identification capability against a set of chemical agents whose vapor pressure is too low to be detected by conventional measures;

- Increasing Counter-Man Portable Air Defense Systems funding by $49 million to a total of $110 million in the Budget. This program will continue to promote the viability of technical countermeasures for commercial aircraft against the threat of shoulder-fired missiles by improving reliability and affordability.

V. Creating a 21st Century Department

The Department has made significant progress in strengthening the management of its business processes from inception to implementation. The Office of the Under Secretary for Management focuses its efforts on the oversight, integration and optimization of the Department's human capital, information technology, financial management, procurement and administrative operations. Over the past year, this office has made strides in designing, planning, and supporting new standards for business processes and resource allocation in order to achieve a cohesive organization while ensuring maximum return on investment. This organization is focused on establishing the overall framework, developing management methods, and monitoring the progress of each management function.

Examples of major enterprise initiatives included in the Budget that contribute to Creating A 21st Century Department include the following:

- The program for electronically managing enterprise resources for government effectiveness and efficiency – or eMerge^2 – to continue implementation of a DHS-wide solution that delivers accurate, relevant and timely resource management information to decision makers. The Budget includes $30 million for this program. By delivering access to critical information across all components, the Department will be able to better support its many front-line activities. It focuses on the areas of accounting and reporting, acquisition and grants management, cost and revenue performance management, asset management and budget that will be integrated with MAX ^{HR}.

- MAX ^{HR} funding of $53 million involves designing and deploying a new human resources system. The $53 million is requested to support the development and deployment of the new HR personnel system as published in the Federal Register on February 1, 2005. These funds will be used to fund the detailed system design for our labor relations and pay-for-performance programs, provide appropriate training and communication for our managers and employees and to provide proper program evaluation and oversight. In this effort, our goal is to create a 21st Century personnel system that is flexible and contemporary while preserving basic civil service principles and the merit system.

- The Information Sharing and Collaboration (ISC) program will affect the policy, procedures, technical, business processes, cultural, and organizational aspects of information sharing and collaboration, including coordinating ISC policy with other federal agencies, drafting technical and operational needs statements, performing policy assessments, and analyzing new requirements. The total funding for FY 2006 will be $16.482 million.

These initiatives will help move the Department toward an efficient and effective shared services environment, avoiding duplication of effort across the program areas.

Conclusion

Two years ago, Congress and the President took on the enormous undertaking of creating a new Department whose central mission would be to secure the homeland. Under Secretary Ridge's leadership, the entities that now comprise the Department of Homeland Security unified under this overarching goal. As I have become acquainted with the many talented people of the Department, I am impressed by all that they have accomplished thus far. But there is no time to pat ourselves on the back.

As the Department initiates our second stage review, organizes around missions, eliminates duplications, and adopts a risk-based approach, we must identify our cross-cutting functions and ensure that we are thinking innovatively how to best exploit our intelligence capabilities, develop policy functions, execute our operational tasks, and implement our long-range preparedness planning.

I thank the Congress for its support, which has been critical in bringing us to this point. I am grateful to be here today to talk about the work we are doing to make America a safer home for us, for our children and generations to come. Thank you for inviting me to appear before you today. I look forward to answering your questions.