Testimony of

The Honorable Tom Ridge

Secretary
Department of Homeland Security
June 9, 2004

WRITTEN TESTIMONY FOR SECRETARY TOM RIDGE
U.S. DEPARTMENT OF HOMELAND SECURITY
to the
Senate Judiciary Committee
June 9, 2004

Good morning, Chairman Hatch, Senator Leahy, and members of the Committee. I am pleased to have the opportunity to address you today on our progress at the Department of Homeland Security and our efforts in leading the national effort to help secure our country.

As we know too well, despite our nation's successes in the global war on terror, our enemies are still dangerous and more determined than ever to attack us here at home. We must be equally determined to stop them, to protect Americans and the American way of life.

In the aftermath of September 11th, President Bush and the Congress worked together to prepare our country for the future. They created the Department of Homeland Security to provide a central point of command for the protection of our country and citizens. On March 1, 2003, we opened our doors with the combined efforts of 180,000 people and 22 agencies, together under a common mission and focused on the President's vision for a safe and secure America.

In order to accomplish our goals for this new Department, we built bridges to one another, ones that interconnected capabilities and people, ones that invited, rather than impeded, two-way channels of communication. We knew from the outset that our vast scope of protective measures had to build upon our existing strengths but, more importantly, be reconstructed in a way that unified and facilitated speed, openness, and easy access for all those involved in the hard work of securing this country every day.

Presidential initiatives, like the USA PATRIOT Act and others, began tearing down the walls that prevented our policy makers from having the benefit of intelligence analyses that were based on all available information. That's just one of the Patriot Act provisions that are so vital to the continued ability of the Department of Homeland Security to work to prevent terrorist attacks and of the reasons why I so strongly support the President's call for Congress to renew those provisions of the Patriot Act that will otherwise expire next year. These tools are important as we build more integrated and coordinated homeland security, intelligence, and law enforcement communities.

We began eliminating roadblocks that once prevented communication between the Federal government and our partners in states, cities, counties and towns across America. Now, we are

replacing them with an active, multi-layered communication system between all levels of government.

We began to connect once disjointed pathways between preparation and prevention. Now, we are establishing a cohesive strategy that combines vulnerability and threat assessment with infrastructure protection.

We began to confront old obstacles that divided the tremendous capabilities of thousands of security professionals from policemen to sheriffs and firemen to EMTs. Now, we are enhancing the abilities of first responders with interoperable standards for communications and equipment.

We began to fully integrate and coordinate our efforts at the national level, paving the way for the Department of Homeland Security as the national focal point for security and protection.

***

The President created the Department of Homeland Security not only to tackle existing tasks, but to recognize and develop new and better methods for accomplishing the job of homeland security and to develop initiatives and systems that we have never taken - or needed to take - to protect our country.

One of the most important "new measures" we have deployed is the integration of the Department into the new homeland security, intelligence, and law enforcement communities that the President has developed in the post-September 11th world.

The establishment of the Department of Homeland Security has created a new analytic capacity, combining specific threat information and actionable intelligence. This new capability allows us to share important information with those who need it most, individuals at the state and local levels.

Let me be clear, the Department of Homeland Security is not specifically in the traditional intelligence collection business - although many of our components collect significant amounts of information - but we are in the analysis and application business. We turn this information into actionable intelligence, which we then disseminate to those who need it most - at the state and local levels.

We interface with all components of the Intelligence Community, including the Terrorist Threat Integration Center (or TTIC), in order to synthesize, analyze and apply information collected from thousands of sources, from electronic surveillance to human reporting.

For instance, our National Targeting Center looks at information from both internal and external sources - such as passenger information and cargo manifests - and combines it with intelligence and threat information. To this end, I am happy to report that DHS has just signed an important agreement with the European Union that permits the legal transfer to DHS of advanced passenger name record (PNR) data from airlines flying between EU countries and the United States. The National Targeting Center uses PNR data in combination with a host of other passenger, cargo intelligence and threat information to conduct a risk analysis that helps to

identify potential terrorists and terrorist targets for additional scrutiny. During the period of heightened alert last December, the targeting center played a pivotal role in analyzing passenger manifest information related to several international flights that were determined to be at risk, in order to ensure that passengers on board did not pose risks to the flights.

Information from the Intelligence Community is not the only kind of information with which we deal. Every day, the Department is sharing important information with homeland security partners across the Federal government and throughout the country at the state and local level. For example, we coordinate our visa and foreign traveler policies with the Department of State; through the FBI, we alert law enforcement personnel and homeland security directors to threat information; we work with fire chiefs and emergency managers on procedures and potential forms of attack; and combat computer viruses with Chief Information Officers in the private sector and governments at all levels.

The Department has made information sharing the hallmark of our new approach to homeland security - and we have developed new tools for communication that reach horizontally across Federal departments and agencies and vertically to our partners at the state, local, territorial, and tribal levels as well as the private sector.

Under the umbrella of the Homeland Security Advisory System, the Department is working to improve coordination and communication among all levels of government, the private sector, and the American people.

This communication tool includes the color-coded Threat Condition, as well as several products that allow us to tailor specific information for specific recipients - a part of the country or an individual sector.

The Department issues Threat Advisories, which contain actionable information about an incident or threat to critical infrastructures, networks, or resources; and Information Bulletins, which impart less-specific information about terrorists' general tendencies, tactics, or strategies and are usually not specific about time or place. This communications process - which represents the first ever centralized effort of its kind in the Federal government rather than relying on the fragmented system that existed before - not only outlines threats, but also recommends specific steps that can be taken to heighten readiness or improve physical protections.

Let me share with you a couple of examples of bulletins that were sent to the front lines - issued to first responders across the country that can use the information to secure our hometowns. A recent bulletin titled "Potential Terrorist Use of Official Identification, Uniforms, or Vehicles" noted that "al-Qaida and other terrorist groups likely view the theft or other illegal acquisition of [these items] as an effective way to increase access and decrease scrutiny in furtherance of planning and operations."

And another bulletin last year regarding "July 4th General Awareness" recommended that facilities heighten security forces, maintain irregularly timed security sweeps, and conduct thorough identity checks.

Of course, this is just a sampling of the information we make available to security professionals across the country. Over the course of our first 14 months, the Department has issued more than 90 alerts and advisories to the American public, Federal, state, and local governments, or the private sector. Together with the response from our partners across the country, they are constantly helping to improve our security posture.

It is important to note that communication is a two-way process - not an information blast, but a true exchange. We collect information from the field and listen to what our partners need from us in order to do their jobs better. This means heightened awareness, better intelligence, wiser decisions, and improved coordination at every level. To that end, we have created several new two-way channels of communication, including the National Infrastructure Coordination Center (or NICC) - created for the private sector - and the Homeland Security Information Network (or HSIN) - created for use by government entities.

The NICC provides a centralized mechanism for the private sector, industry representatives, individual companies and the Information Sharing and Analysis Centers - or ISACs - to share and receive situational information about a threat, event, or crisis. The NICC also supports the Homeland Security Operations Center - a 24-hour, 7-days-a-week nerve center that enables the Department to monitor activity across the country. Obviously, this tool would not be effective without the participation of our partners across America.

One of the ways we receive this input is through the recently launched Homeland Security Information Network (HSIN). This real-time collaboration system is already used by more than one thousand first responders, mainly from the law enforcement community, to report incidents, crimes and potential terrorist acts to one another and to the Department through our 24-hour Operations Center.

It was developed by state and local officials in partnership with the Federal government. It allows multiple jurisdictions, disciplines and emergency operation centers to receive and share the same intelligence and tactical information - so that those who need to act on information have the same overall situational awareness.

Through the Homeland Security Information Network, we are expanding our connectivity and counterterrorism capabilities to two new communities - senior decision makers such as Governors and Homeland Security Advisors and Emergency Operations Centers.

In addition, the information network will eventually provide these collaborative and analytic capabilities to all 50 states, territories, tribal governments and major urban areas. By the end of the year we will achieve real-time nationwide connectivity.

In fact, by this fall more than 5,000 officials will be linked through the Homeland Security Information Network. Every homeland security advisor will have access to the information network, as will Governors, Adjutants Generals, state and urban Police Departments, and Emergency Operations Centers across the country. And by year's end, we will be able to share classified information up to the "Secret" level, and provide training for sensitive information

management and use. Over time, the full suite of applications on the information network will be available on the robust national classified information sharing system that we are developing.

In the future, with our state and local partners, we will expand this information sharing environment - while continuing to safeguard classified information - to an ever-widening circle of first responders for ever-increasing layers of coordination and communication between those tasked with protecting our homeland. In short, the Homeland Security Information Network will be both user-friendly and used by more of our partners.

It's important to note - this is a tool of prevention. The main goal of this network is to stop an attack before it ever comes to fruition. Through this system, states will be able to immediately communicate to their county and local partners - creating their own communications networks. And in the future, the private sector will be able to access the system so they can coordinate their preparedness efforts with ours.

During last year's blackout we concluded early on through local reporting to this information network that terrorism was not a likely cause. And more recently, we were able to dispel rumors of evacuations from government offices in Washington, D.C. This capability saves cities countless man hours and precious dollars.

The Homeland Security Information Network communities have also been the cornerstone of our efforts to protect our national monuments and secure holiday celebrations and special events such as the Super Bowl and this past New Year's Eve celebrations. I have watched first hand as state, county and city Operations Centers from across the country went on-line, sharing information and viewing the same operational picture in real time.

Just as important, improvements in our communication - and cooperation - are not limited to the domestic front. During last year's Christmas holiday period, we were able to communicate quickly and effectively with security officials on the ground in England, France and Mexico to recommend and implement plans to mitigate terrorist threats to airline passengers traveling to the United States.

This is an example of the tangible results we have produced by focusing our efforts on effective two-way communications. Here at home, for instance, field agents guarding our Nation's borders stop individuals when necessary based on information provided by the Department and, in return, report back to headquarters with information that can be analyzed for helpful intelligence. The head of my intelligence analysis unit even spoke directly with a state trooper in Wyoming after a routine traffic stop - in order to clarify potential threat information.

***

Some of the most important pieces of intelligence or information that we receive have to do with potential targets. Once we take into account all of the information that is available, we are using a risk management strategy to anticipate threats, protect our infrastructure, and prevent attacks.

The responsibility is great, and the practical challenge is even greater. We share nearly 7,500 miles of land border with Canada and Mexico, across which more than 500 million people, 130

million motor vehicles, and 2.5 million rail cars pass every year. We patrol almost 95,000 miles of shoreline and navigable waters, and 361 ports that see 8,000 foreign flag vessels, 9 million containers of cargo, and nearly 200 million cruise and ferry passengers every year.

We have some 445 primary airports and another 124 commercial service airports that see 30,000 flights and 1.8 million passengers every day. There are approximately 110,000 miles of highway and 220,000 miles of rail track that cut across our nation, and 590,000 bridges dotting America's biggest cities and smallest towns.

That is just a thumbnail of the vast infrastructure that supports the largest and most efficient economy in the world - with more than $11 trillion in Gross Domestic Product.

Of course, we cannot protect all of it, every single day, against every form of attack. We must find a way to strike the right balance between protection and progress. As a result, for the first time, we are employing a risk management methodology to prioritize our efforts. It doesn't mean that we are giving up on one area in favor of another. It means that we are trying to be as analytic and efficient as possible to keep ahead of our terrorist enemies.

We are employing our improved two-way communications as an integral aspect of the first of five steps in our new risk management methodology. In the first step, we determine which targets might be most attractive to terrorists, including key resources and sectors such as the Internet, telecommunications, nuclear and chemical facilities, water, energy, and transportation systems, banks and financial centers, and national - or natural - monuments, icons, and treasures. We do this, as I mentioned, by collecting vast amounts of data from our partners.

Next, we assess the vulnerabilities of these sites - whether they have good security systems, effective counter measures in place, or strong defenses against entry and infiltration. Third, this information is analyzed according to the threat environment that exists - including information from the intelligence community - and prioritized to determine which sites or sectors pose the greatest risk. We then use this information to strategically build or bolster protective measures and, lastly, evaluate our progress.

The threat environment surrounding our critical infrastructure changes by the hour - even the minute. We recognize that our enemies are nimble, clever, and extremely persistent. They are able to evaluate our security measures and develop new methods of attack, on new sectors and assets, and in new areas of the country. As a result, our priorities can - and must - change quickly. Today's highest risk sector might be tomorrow's lowest priority - and vice versa.

That is why we are developing a National Infrastructure Protection Plan (NIPP) in coordination with our partners across the public and private sectors, as mandated by President Bush in his Homeland Security Presidential Directive Seven (HSPD-7). By the end of this year, the final NIPP plan will outline a consistent baseline for protection standards and protective measures for each sector of critical infrastructure. This will guide the actions of Federal agencies, state and local governments, and private sector owners and operators, helping them move toward prioritized and consistent levels of protection against terrorist attacks across all of our critical infrastructure sectors.

This process of integrating widespread protection efforts with a dynamic, real-time map of vulnerable critical infrastructure has never been done before on the national level. We are working to make it an effective tool throughout the Department of Homeland Security.

***

The combination of new abilities in information sharing, improved two-way communications, and our unique infrastructure protection plan has given the Department capabilities that the Federal government has never had before. Most importantly, it means we can act to prevent terrorist attacks and protect Americans. We have emerged from a static security environment into a dynamic, real-time, action-oriented system of layered protections...on air, land, and sea.

Before the Department was created, America's homeland security functions focused largely on law enforcement and interdiction. Today, strong action and decisive leadership dictate the steps we take to implement protective measures or respond to various threats. We have greatly enhanced our overall capability to act - and we do so at three strategic levels: operational, tactical, and incident driven.

Every day, our job is to work to make our country more secure, so during our normal operations, we protect infrastructures or geographic areas as a result of non-specific strategic threats. I would like to emphasize that our normal operations mode still represents a higher level of alert and a greater commitment to vigilance than has ever existed in the Federal government. We are constantly evaluating our intelligence, our inventory of infrastructure, and a threat environment that literally changes by the hour and day.

Even in this ever-changing environment, however, we believe that terrorists will consistently target certain sectors and consistently look to use certain types of attack. That knowledge allows us to operate at a high level of awareness, even in our normal mode. As a result, we place special emphasis on these sectors in our daily operations, and by the end of this year we will have increased security in many of the highest risk areas.

We also think that terrorists will continue to attempt to utilize airplanes and other transportation systems as weapons of mass destruction, so we integrate this knowledge into our ongoing efforts to shore up vulnerabilities in our transportation sector. Earlier this year, we worked closely with metropolitan transit police departments to raise awareness of the threat of attack on transporters of "toxic inhalation hazard" materials, which could expose populations to hazardous chemicals carried in rail cars, and worked closely with other federal agencies to recommend and begin implementing protective actions to reduce this vulnerability. In a separate effort during the Holiday alert period, we have worked closely with industry and the Department of Transportation to study all existing security gaps and are currently designing a risk mitigation strategy to reduce these risks. We have issued security directives to metropolitan transit agencies, commuter and passenger rail operators requiring that they implement protective measures to counter the threat of attack to the passenger rail system. And for the long term, we have begun to work with the private sector to design and develop more secure rail cars for carrying toxic chemicals.

If we receive threat information for specific cities or sectors, information on which we can take action, we move from our normal stance into the tactical operation mode - a new dimension of protection unique to the operations of the Department. At this point, we increase or accelerate protective measures at the site of these targets.

Lastly, as we saw during the period over the holidays when the threat level was raised to Orange, we have the ability to operate in an incident-driven mode. In this case, we act quickly on reliable intelligence about a specific city, building, event, or type of attack. For example, just last month, we discovered a critical vulnerability in some of the routers that control much of the global Internet infrastructure. If exploited, this security gap could have caused a large-scale disruption to the operation of the Internet, impacting the economy and security of the United States and nations around the world. However, DHS, in cooperation with several private sector firms and government agencies, was able to quickly disseminate a warning and patch for this vulnerability through the U.S. Computer Emergency Readiness Team - or U.S. CERT. In this case, we reduced a global security risk in a matter of hours.

In this situational mode, the Department draws on all of the new capabilities I have just outlined for you - heightened DHS involvement in analyzing intelligence, widespread coordination at the Federal level, and intense two-way communications. This is when the hard work of early preparation and active engagement pays dividends.

Let me give you a sense of what this actually looks like.

On December 21, 2003, I announced to the public that we had raised the Threat Condition from an Elevated to High risk of terrorist attack - or from Code Yellow to Code Orange.

Before the decision was made to raise the level, the Intelligence Community received a substantial increase in the volume of threat-related intelligence reports. Credible intelligence sources suggested that there was the possibility of attacks against the homeland around the holiday season, a possibility that appeared to be greater at that point in time than at any moment since September 11th. The information we received indicated that extremists abroad were anticipating near-term attacks that would rival - or exceed - the scope and impact of those we experienced in New York, at the Pentagon, and in Pennsylvania on September 11th.

This collection of information and intelligence was enough to warrant a nationwide alert, and that is what we did by raising the Threat Condition to Orange - which is designed to trigger a series of protective actions by homeland security professionals across the country. We briefed the nation's Governors, Homeland Security Advisors, Mayors, and other local officials and asked them to review the security measures they had in place, and advised them to increase protections to thwart terrorist attacks.

This was the beginning of three weeks of consistent two-way communications between the Department and our partners throughout the country. Our Office of State and Local Government Coordination was in constant contact with homeland security officials in states, cities and counties across America and received routine periodic updates from higher risk areas on the protective measures they were implementing to keep citizens and infrastructure safe from attack. Our Office of Private Sector Liaison reached out to several thousand companies and

organizations with the Department's instructions for heightened alert and increased vigilance. And our 24-hour Homeland Security Operations Center - and Interagency Incident Management Group - fielded thousands of calls during this period and shared vital information with our national and international partners.

The response around the country to this call to action was exceptional. There was an increased police presence at shopping malls, train stations, power plants, and large gatherings such as sporting events and holiday celebrations. Emergency communications plans were implemented and watch centers were activated. We increased our detection capabilities by deploying sensor equipment in different parts of the country, including expanding our BioWatch program. We took important steps to ensure coordination at every level, such as placing local law enforcement personnel in our headquarters command center, providing air marine assets to several major events, and sending DHS personnel to monitor actions on the ground in areas of special attention across the country. And we encouraged individual citizens to review - or develop - their family emergency plans or Ready Kits. We implemented broad security measures and, when the situation warranted, we recommended and, in some cases, carried out ourselves, targeted actions such as grounding high-risk flights headed for the United States from overseas.

We know that greater security plus added vigilance is a deterrent; and, thankfully, this time of heightened alert passed safely and without incident. Each time we raise the Threat Condition, which we have now done five times since August 2002, we learn more about the process and improve our abilities to communicate and coordinate effectively with the public, with the private sector, and with our partners at every level of government.

As these examples show, the Department of Homeland Security operates at the strategic, tactical, and situational level every day - moving seamlessly between them as the situation dictates. By having a single integrated department, we have leveraged tremendous resources and created capabilities that never existed before September 11th.

***

Another area where major changes have been implemented is in the way we welcome people to our country. The experience of traveling to the United States has changed for millions of foreign visitors over the past two years. The U.S. government has created new procedures, laws and travel regulations, stepped up the enforcement of existing laws and processes, and - in creating the Department of Homeland Security - restructured many travel processes, functions, requirements and responsibilities. And more changes are coming. Over the next several years, Homeland Security will continue to enhance its systems and introduce new elements to the international travel experience.

As a result, the challenge of creating awareness, understanding and support for U.S. travel policies among diverse publics has increased substantially. The United States today finds itself struggling to catch up with these changes and, in many cases, to ameliorate unfavorable attitudes and perceptions about traveling to the United States.

Our policies have been designed to keep our borders closed to terrorists but open to legitimate, law-abiding visitors. They deserve to travel on secure airlines and vessels; to be processed efficiently through our ports and border crossings; and to have their privacy respected and protected from abuse. And once here, they deserve to live in safety -- not in fear of terrorists,

criminals and fugitives from the law. That is the charge of our open, welcoming nation -- a champion of freedom at home and abroad. I believe the changes we favor will help us preserve those freedoms and protect all individuals from harm.

Currently, 27 nations are members of the Visa Waiver Program, or VWP. Under the program, citizens of participating countries are allowed to travel to the United States for tourism or business for 90 days or less without obtaining a visa.

The policy encourages travel and trade between the United States and our allies. However, one unintended consequence of the policy is a potentially significant gap in security as those wishing to avoid visa security checks conducted at U.S. consulates abroad attempt to take advantage of the program.

One of the responsibilities of the Department of Homeland Security, in consultation with the Department of State and other relevant agencies, is to determine whether the continued participation of a particular nation in the VWP poses a threat to the national security or law enforcement interests of the United States, and therefore should be ended.

The Enhanced Border Security and Visa Entry Reform Act requires that beginning on October 26th, 2004, Visa Waiver Program countries have a program in place to issue their nationals machine-readable passports. They must be tamper-resistant and incorporate biometric and document authentication identifiers that comply with International Civil Aviation Organization (ICAO) standards.

The law also requires that visitors coming to the United States under the VWP present these new biometric and machine-readable passports if they were issued on or after that date. VWP travelers with non-biometric passports issued after 10-26-04 will need a visa to enter the United States.

Extension of the Deadline

We have learned that while most Visa Waiver Program countries will be able to certify that they have a program in place to issue biometric passports by the October 26th deadline, few, if any, of these countries will actually be able to produce biometric passports by that date.

Under the current deadline, millions of visitors from Visa Waiver Program countries who do not have ICAO-compliant passports will have to obtain visas prior to traveling to the United States. As my colleague Secretary Powell has indicated in a hearing last month, this sweeping change will place a great burden on our consulates and have significant negative implications on tourism, travel and commerce. So relief is critical. Secretary Powell and I are extremely encouraged by the progress that has already been made by Visa Waiver Program countries to meet the emerging ICAO standards. We will continue to work with them to help them meet the mandatory deadlines. It must be noted that the reason these countries cannot meet the October 26th deadline is not a lack of will or commitment, but rather challenging scientific and technical issues.

For those same technical reasons, the Department of Homeland Security is not currently in a position to acquire and deploy equipment and software to biometrically compare and authenticate those documents. Further, adhering to the original deadline also would likely prevent us from creating a system that is interoperable for all nations. Like the foundation of a house, interoperability must be built into the system from the very beginning. To do otherwise would prove extremely expensive, time-consuming and difficult.

Acknowledging the current limited state of technology and the potential for harm to our relations with our closest allies, the Department, as stated earlier, requests that the October 26th, 2004, deadline under the relevant sections of the Enhanced Border Security and Visa Entry Reform Act

be extended to November 30th, 2006.

The US-VISIT Program

Despite these challenges, we have identified a partial solution that we believe will allow us to improve the nation's security and the integrity of the Visa Waiver Program. This involves enrolling Visa Waiver Program travelers in the US-VISIT system, beginning this fall.

US-VISIT represents the greatest single advance in border technology in three decades. The Department has established US-VISIT to:

? Enhance the safety of our citizens and visitors;

? Facilitate legitimate travel and trade;

? Ensure the integrity of our immigration system; and

? Protect the privacy of travelers to the United States.

US-VISIT represents a continuum of security measures that uses biometrics as a key element. Biometrics such as digital, inkless fingerscans and digital photographs enable the Department to determine whether the person applying for entry to the United States is the same person who was issued the visa by State. Both State and our Department use biometric and biographic data to check against appropriate "lookout" data.

The Department deployed the first increment of US-VISIT on time and within budget. And, as it includes biometrics ahead of schedule, we have exceeded the mandate established by Congress. On January 5th, 2004, US-VISIT entry procedures were operational at 115 airports and 14 seaports. By the end of the year, US-VISIT will be in operation at our 50 busiest land ports of entry. We have also begun pilot-testing biometric exit procedures at one airport and one seaport and will expand to additional pilot locations later this summer.

US-VISIT procedures are clear, simple, and fast for visitors. On average, US-VISIT procedures take less than 15 seconds per person during the inspection process. As of the beginning of May, more than 4 million foreign visitors have been processed.

As impressive as its speed is already US-VISIT has matched more than 300 persons against criminal databases, preventing more than 100 known or suspected criminals from entering the country. More than 200 were matched while applying for a visa at a State Department post overseas.

As noted earlier, we are also dedicated to safeguarding travelers' privacy. We have extended the principles and protections of the 1974 Privacy Act to all individuals processed through US-VISIT. And US-VISIT features a three-stage process for redress if an individual has a complaint.

Visitors to this nation have a right to be secure from criminals and predators. US-VISIT has helped to make that right a reality.

One example: on December 28th, 2003, an international traveler appeared for inspection at Newark International Airport. Standard biographic record checks using a name and date of birth would likely have cleared the individual. However, when his fingerprints were scanned and checked against the US-VISIT biometric database, it was revealed that he was a convicted felon who had been previously deported from the United States. He had used multiple aliases to disguise from authorities his record of rape, assault, criminal possession of a weapon, and the making of terrorist threats.

Similar examples abound. A fugitive drug trafficker was captured after two decades on the run. A traveler sporting three Social Security numbers and a 14-year criminal history was nabbed. And just weeks ago, an airline crewmember was biometrically identified as having been convicted for forgery and violation of electronic funds transfer accounts. Crewmembers are not exempt from US-VISIT. She was sent home and her visa was cancelled.

Through US-VISIT, our two Departments have identified numerous criminal and immigration-law violators who otherwise would have disappeared. Every day the system highlights the importance of using accurate, timely information to protect our nation from terrorists and criminals - and, I would add, to protect innocent non-citizens and their families from being tarred with a broad brush or targeted by mistake. By focusing on individual behavior, US-VISIT and programs like it help reduce our reliance on more arbitrary and unfair standards such as nationality.

VWP and US-VISIT

In FY 2003, the Department of Homeland Security recorded the admission of approximately 13 million Visa Waiver Program traveler visits through air and sea ports of entry.

By expanding US-VISIT to include processing of Visa Waiver Program travelers, the Department expects to double the number of admissions processed through US-VISIT, thus enhancing the integrity of our borders.

I would add that there are some travelers from Visa Waiver countries who are required to obtain nonimmigrant visas, and so have already been successfully processed through US-VISIT. Since its implementation, approximately 400,000 nonimmigrant visa holders from Visa Waiver Program countries have been processed.

Earlier this month we briefed ambassadors of Visa Waiver countries on this change, and overall they are supportive. A European Commission spokesperson told the Wall Street Journal that, "We [will] work closely with the U.S., with whom we share counterterrorism goals, to ensure that any new measures are introduced with minimum disruption and maximum safety."

These Visa Waiver Program countries appreciate our interest in increasing security as well as our support for the deadline extension to enable them to follow our lead.

Many of them, including Australia, the Netherlands, and Singapore, are actively engaged in developing programs that will allow them to collect biometrics and match the data upon a visitor's entry. We are working with many of these countries to share information about terrorism and other security threats, in addition to opportunities for improvements in immigration and border management.

And we are working with Secretary Powell to get the word out that the United States remains an open and welcoming nation to those who wish to live, work or study here.

Yes, this new era demands new security requirements, such as mandatory interviews for visa-holders, small processing fees, and the verification of a student's enrollment status through our Student and Exchange Visitor Information System, or SEVIS, which serves nearly 10,000 campuses across the country.

But it also demands that we extend a helping hand. Our SEVIS "Tiger Teams," for instance, show up at airports as foreign students arrive to help them navigate the process. They serve as on-scene ombudsmen, contacting the universities and trouble-shooting so that legitimate students are not left behind.

US-VISIT is critical to our national security as well as our economic freedom. It is already making a significant contribution to the Department's efforts to provide a safer and more secure America.

We recognize that we have a long way to go. We will build upon this initial framework and solid foundation to ensure that we continue to meet our goals of enhancing our security while facilitating travel for the millions of visitors we welcome each year.

We are committed to a program that enhances the integrity of our immigration system, that catches the few and expedites the many - and, above all, that keeps our doors open and our

nation secure.
Countries in the Visa Waiver Program are our closest allies and economic partners. A two-year extension of the October 26th, 2004 biometrics deadline will permit these allies to remain in the Visa Waiver Program. And processing Visa Waiver Program travelers through US-VISIT will help our two Departments - and nation -- achieve our security objectives.

***

The tools we have developed have now become a formidable force multiplier in the effort to secure and protect America. The first year's accomplishments have provided an excellent foundation for future work - and there remains plenty to do. That is why we have recently completed the Department's first high-level Strategic Plan - which includes vision and mission statements, and a set of strategic goals and objectives that provide the framework for our daily operations into the future.

I'd like to discuss the Department's seven key priorities for the coming year. I think they will provide the Committee with some insight into where our collective homeland security efforts have been and where they are going in the future.

1. Stronger Information Sharing and Infrastructure Protection

Our first goal is to further improve information sharing and infrastructure protection. I have already provided many of the details of our efforts, but suffice to say that we will dig deeper into our efforts - specifically, work in greater tandem with the private sector to strengthen vertical communication systems and significantly increase permanent protections around our nation's most vital assets. The goal is to maximize real-time sharing of situational information - without delay, and with full throttle distribution of intelligence to those in the field who need to act on it.

By the end of this year, we intend to complete vulnerability assessment guidelines for three critical infrastructures: chemical, petroleum and nuclear The Department has been working with industry through the American Society of Mechanical Engineers(ASME) to develop guidelines for each of the eight critical infrastructure subsectors: chemical facilities, nuclear power plants, nuclear spent fuel storage facilities, petroleum facilities, liquefied natural gas storage locations, railroad bridges, subway systems, and highway tunnels. The Department with the assistance of ASME will work to standardize these guidelines as they are vetted through the various infrastructures.

We are building the National Assets Database, a national inventory of physical critical infrastructure that contains thousands of sites and is growing literally every day. This is a dynamic document that is constantly updated to include additional sites based upon the ever-changing threat environment in which we operate.

2. Standards for Interoperable Communications and Equipment

Part of the tragedy of September 11th was that equipment didn't work across jurisdictions and disciplines. Fire department radios couldn't transmit to police department radios. Firefighters rushing in from other cities and even neighborhoods were, in some cases, unable to assist

because the couplings that attach "hoses to hydrants" simply wouldn't fit; they weren't compatible. Our first responders are first on the scene and their ability to communicate and work with each other in the event of a crisis is paramount - and their inability to do so is a long-standing, complex and critical issue facing this Nation.

We are employing a two-track strategy as we work to solve this problem. There are immediate steps the Department can take in the short term, while we focus everyone's attention on a long-term, integrated solution to overall interoperability. Already, for example, the Department has identified technical specifications for a baseline incident interoperable communication system. If adopted at the state and local level, by the end of 2004, most first responders will have a way to communicate with each other during a crisis, regardless of frequency or mode of communication.

The Department also recently announced the first comprehensive Statement of Requirements for communications throughout the first responder community. This set of standards marks the first time in history that 50,000 public safety agencies across the country will have a common standard for wireless communications and interoperability. This will serve as an important tool that will bring governments, public safety officials, the communications industry, and future research and development efforts together under a common mission.

We have also adopted the first set of standards regarding personal protective equipment developed to protect first responders against chemical, biological, radiological and nuclear incidents.

These standards, which will assist state and local procurement officials and manufacturers, are intended to provide emergency personnel with the best available protective gear - allowing them to protect themselves, as they work to protect others.

I am pleased to report that all of the Department's efforts in this area will be coordinated by a new Office of Interoperability and Compatibility. Much of their work has already begun, and they will continue to coordinate and leverage the vast efforts spread across the Federal government to reduce unnecessary duplication in programs and spending, identify and promote best practices, and conduct research and development, testing and evaluation, develop standards, provide technical assistance, training, and develop grant guidance for interoperability between local, state, and federal agencies.

This office will focus not just on interoperable communications, but also on the gear that will be used by multiple jurisdictions - firefighters and police officers from different neighborhoods - as they join together to respond to a major event. In addition, this Office has initiated a program aimed at providing communications interoperability at disaster sites in the near term, and we expect multiple cities to achieve this goal sometime this fall.

These immediate steps at the Federal level will begin to build a foundation for longer-term efforts and a truly national solution.

This second track will require actionable results at the state and local level - in other words, a resolve not to let an incompatible radio frequency or a too-small/too-large piece of safety equipment impede the ability of brave men and women to save the lives of citizens...as well as

their own. A truly nationwide interoperable system demands commitment from leaders at all levels - and we are already beginning to see a commitment to this important principle.

3. Integrated Border and Port Security Systems

The President quickly acted to strengthen security at our borders - welcoming the free flow of trade and travelers, while keeping terrorists out. We unified the inspection process - presenting "one face" at the border - and in doing so, nurtured better morale, improved service, and reduced delays. One face at the border streamlines our personnel and our processes, joining customs, immigration, and agriculture inspectors together under one chain of command, one set of rules and guidelines, and one multi-faceted training program. Today, our Customs and Border Protection Officers are being prepared for all three elements of border enforcement.

The President took immediate and extensive measures to enhance aviation security. In less than a year, America deployed newly trained screeners and thousands of Federal air marshals, hardened cockpit doors on aircraft, and introduced state-of-the-art technologies, which, from the curb to the cockpit, have made airline travel safer.

We launched the US-VISIT program at 115 airports and 14 seaports across the country. Now, the "smart technology" of biometrics is speeding the entry of millions of travelers, and stopping criminals before they enter our country. To date, more than 4 million passengers have been processed through US-VISIT, and more than 400 passengers have been apprehended or prevented from entering the country, including one prison escapee who had been on the run for more than 20 years and another man with 8 aliases who managed to enter the country in December, but was stopped by US-VISIT when he tried to enter again just two months later.

With the help of the FBI and other federal partners, together we also stood up the Terrorist Screening Center to give law enforcement a one-stop shop for information on terrorist watch lists. The screening center continues to make great strides toward total watch list consolidation; and already we are able to share lists with our border officials at all ports of entry - land, air, and sea - and with state and local law enforcement through the National Crime Information Center - or NCIC.

We also looked at our system for welcoming foreign students, retooled it, and by last fall had a new system in place that ensures that legitimate foreign students are not delayed upon entry - and that those posing as students, seeking fraudulent entry to schools, are stopped in their tracks. Last fall almost 300,000 students were successfully cleared for study at our institutions of higher education. Those two hundred who attempted entry, but were not registered at any school, were sent home.

We significantly expanded the nation's container security initiative, known as CSI. The result: there are DHS inspectors in Rotterdam, in Singapore, in Hong Kong, and 14 other international ports of trade, working alongside our allies to target and screen the nearly 20,000 containers of cargo that arrive from these ports at our shores every day.

To further improve upon the base of border and port security protective measures which we have already established, we will expand the US-VISIT program to our 50 busiest land ports of entry

by the end of this year, and add an additional seven Free and Secure Trade lanes, bringing the total to 18 locations.

We will expand the NEXUS and SENTRI trusted traveler programs to expedite the passage of frequent, low risk border crossers that undergo a background check.

We will strengthen the critical partnership with private sector owners and operators of the supply chain through expansion of the Customs Trade Partnership Against Terrorism, which provides business incentives to companies that voluntarily meet a set of government-approved security standards. More than 6,000 importers, carriers, and brokers, including 186 foreign manufacturers, are now enrolled in C-TPAT.

With private sector involvement and support, we will also enhance air cargo security by investing in new research and technology, and expanding pre-screening and known-shipper programs.

We also will deploy aerial surveillance and sensor technology, increase manpower and interagency coordination at specific points along the border, expand the Container Security Initiative to 10 additional high-volume ports, and work with the private sector to facilitate compliance and assessment of new maritime security regulations.

4. Create More Prepared Communities

Since March 1 of last year, we have allocated or awarded a record $8 billion to states, regions and cities to help train and equip our Nation's dedicated first responders.

Now, we want to examine as many ways as possible to broaden communication and coordinate actions, so that when people show up at an incident; they're not meeting for the first time; they're not confused about the chain of command; and they're not lacking for help in their communities as they scramble to aid and assist our citizens in the midst of a crisis.

As part of this effort, we introduced the National Incident Management System - or NIMS - so that those with responsibility for protection at all levels of government and the private sector understand what their role will be - and will have the tools they need to be effective.

NIMS is the Nation's first-ever standardized approach to incident management and response - and it unifies Federal, state, and local lines of government into one coordinated effort.

NIMS makes America safer - across our entire Nation and throughout every neighborhood - by establishing a uniform set of processes, protocols, and procedures that all emergency responders, at every level of government, will use to conduct response actions.

For the first time, all of the Nation's emergency teams and authorities will use a common language, and a common set of procedures when working individually - and together - to keep America safe.

The Department is also developing the National Response Plan to integrate all of the current Federal response capabilities under a single "all hazards" system for prevention, preparedness, response and recovery.

The plan is being developed with guidance from all stakeholders - Federal government agencies, state, local, and tribal officials, as well as first responders. This working blueprint will enhance current Federal capabilities and will unify the team that will be charged with responding to potential attacks or disasters.

We are also building a foundation on which the private sector can take important steps to improve their readiness. The ANSI/NFPA 1600 - a set of voluntary standards developed by the American National Standards Institute and the National Fire Protection Association - empower the private sector to examine their own readiness and take part in the shared responsibility of homeland security. These standards encourage mutual respect, cooperation, and open communication - essential elements of our national approach to readiness. Voluntary standards like these - and the process used to develop them - help make us smarter about how to perform our duties better, and give us direction and guidance in the areas we need them most. They are just one tool - but an important one - in our effort to make our country more secure.

Citizens are just as integral to combating terrorism as any state and local government or private company. Terrorism is insidious. Terrorists seek to infiltrate our society, scope out targets, and wage war in our streets and cities.

And so, to achieve a national movement toward an integrated and seamless degree of protection, it's vital that we continue to reach out to our citizens and empower them to play a direct role in securing their families and their communities.

The Department of Homeland Security will focus its efforts on raising the baseline level of preparedness across the Nation.

We will continue to educate the public about the importance of being prepared for all emergencies, whether wrought by disaster or design. Our goal over the next year will be to accelerate the basic level of citizen preparedness across the Nation. Current research suggests that between 20 to 30 percent of Americans have an emergency supply kit and that 15 percent have a communications plan.

Our desire is that nearly half of all Americans, in some form or combination, will be better prepared by the end of 2004 - whether that's by preparing family Ready kits and emergency plans; volunteering to aid in disaster planning; or engaging in CPR and training exercises to help someone in a life-threatening situation.

To help push this forward-leaning agenda, by the end of 2004, we will add to the strength of our existing Ready campaign by launching two new citizen preparedness endeavors -- Ready for Business and Ready for Schools. We will also continue to work with third party organizations, such as The American Red Cross and America Prepared - and, of course, Citizen Corps. Citizen Corps' mission is to encourage everyone to participate in making America safer; their councils,

which have grown to more than 1,100, have helped us deliver the Ready message at the grassroots level - the level where it's needed most.

5. New Technologies and Tools

Every day we must operate with the knowledge that our enemies are changing based on how we change. As we shore up one vulnerability, they work to uncover another. This is why science and technology is key to winning this new kind of war. The work we do at Homeland Security, in partnership with the private sector, national laboratories, universities and research centers, helps us push the scientific envelope. It helps drive the development and use of high technology to combat the weapons of high consequence. New tools of analysis, information sharing and detection can help us counter terrorist attacks -- before they can happen -- and if they happen, minimize their impact.

For instance, we are developing new capabilities for detecting the presence of nuclear materials in shipping containers and vehicles. We are also developing the next generation of biological and chemical detectors, ones uniquely sensitive enough to not only alert people to the presence of dangerous pathogens, but allow for evacuation by redirecting air flow.

We also established our first three Centers of Excellence and our first class of Homeland Security Scholars and Fellows -- to foster new thinking, new capabilities and new career paths that are so essential to the fight against terrorism.

These capabilities are critical to a war where speed of knowledge and action is vital to the protection of the public. Homeland Security can't drive these advances, only science can, but together with our partners we are taking up the charge to secure our country using the latest technologies available.

6. Improved Customer Service at Immigration Services

Another key priority of this department will be to improve and protect immigration practices, and at the same time improve homeland security. Again, it is part of our mission to ensure that we remain a welcoming nation for people who want a better way of life and who want to make a contribution to the great American story - but also to keep our borders and communities closed to terrorists.

Citizenship has long been among the most important privileges this Nation can bestow. And, as the Department that oversees this critical function, we are committed to making the immigration and naturalization process a welcoming and timely one. Our four new pilot programs - two in the Los Angeles area, Dallas and New York City - are aimed at reducing the backlog of pending cases and streamlining the citizenship process, while strictly protecting the privacy and civil liberties of everyone involved. Already in Dallas, the project called the I-130 Pilot has been a proven success. This customer service initiative aims to complete the "adjustment of status" process within 90 days. In Los Angeles, the I-90 pilot aims to reduce the wait time to replace or renew a permanent resident card or green card from a year to less than a week.

We will soon expand our E-Filing initiative, allowing applicants to complete several of the most

popular forms online. Last year E-Filing began with two forms - an application to replace a green card and an application for employment authorization. Soon this customer service initiative will support eight forms that account for more than 50% of the applications for benefits filed each year. The new forms will include the application for Temporary Protected Status, employment based petitions and change of status. By the end of fiscal year 2006, E-Filing will include a total of 12 forms that will account for more than 90% of the applications for benefits filed yearly. We have also posted processing times - updated monthly - for forms on the United States Citizenship and Immigration Services website.

CIS is also creating an orientation guide to help immigrants better integrate into American society. This guide will introduce local community resources, emergency service providers, and a host of critical information to new residents in our country.

7. Build a 21st Century Department

We're working to build a department that strives to create the model government agency for the 21st century. In a 21st century threat environment, nothing less will do. Of course, just getting up and running operationally was a challenge unto itself - merging 180,000 people, 22 Federal entities, 22 different human resources servicing offices, 8 different payroll systems, 19 financial management centers, and 13 procurement systems.

We have proposed a new human resource system - called MAX HR - which will allow the Department to act swiftly and decisively in response to our mission needs, quickly adapt to the changing nature of our work, and attract, maintain, and motivate a highly skilled workforce.

New provisions include pay for performance and performance management, while preserving labor relations, appeals processes, and protecting the rights and responsibilities of all workers.

The Department has undertaken a resource transformation initiative entitled eMerge2 which is a business-focused program that seeks to consolidate and integrate the Department's budget, accounting and reporting, cost management, asset management, and acquisitions and grants functions.

We have also instituted a Leadership Development Curriculum that includes "One-DHS" training and candidate development to ensure that our workforce is marked by outstanding leadership and guided by a singular commitment to success.

Today, we operate as a single unit - one team, one mission, one fight. And our management philosophy and leadership development reflect that.

***

The entire Department, in fact, reflects this shared responsibility. We are committed to leading the unified national effort to secure America. We have done so - and will continue to do so - by developing new and innovative methodologies to prevent and deter terrorist attacks, and protect against and respond to threats and hazards. All the while, we will ensure that we maintain safe

and secure borders, welcome lawful immigrants and visitors, and promote the free flow of commerce.

Homeland security is not one department or one organization. Homeland security is about building bridges between the people tasked with our Nation's protection, and giving them the tools they need to do their jobs well.

Homeland security is about the integration of a nation, the integration of people and technology to make us smarter, more sophisticated, and better protected.

The entire Department, in fact, reflects this shared responsibility. We are committed to leading the unified national effort to secure America. We have done so - and will continue to do so - by developing new and innovative methodologies to prevent and deter terrorist attacks, and protect against and respond to threats and hazards. All the while, we will ensure that we maintain safe and secure borders, welcome lawful immigrants and visitors, and promote the free flow of commerce, and accomplish these goals in a way that is respectful of the civil liberties and personal privacy of our citizens and our visitors.