Press Office
U.S. Department of Homeland Security

Press Release

December 12, 2007
Contact: DHS Press Office, (202) 282-8010

REMARKS BY HOMELAND SECURITY SECRETARY MICHAEL CHERTOFF ON 2007 ACHIEVEMENTS AND 2008 PRIORITIES

SECRETARY CHERTOFF: Well, thank you for your warm welcome. I'm honored to be here today. I also want to thank Chairman Hamilton for his very gracious introduction. If I can reciprocate with the praise for a moment, our nation owes you a debt of gratitude for your service on the 9/11 Commission, on the Iraq Study Group. In every way you've contributed to our national security, not only in your service for many years as a member of Congress, but in your service for the years since you've been a member for Congress -- truly a wise man in the classic mode.

I'd also like to welcome distinguished guests, fellow colleagues, some former colleagues I see, friends, alumni of the Department, and members of the media.

As Chairman Hamilton said, I am coming up on the third anniversary of my being sworn in as Secretary of Homeland Security, and we are at the end of another year of operations for the Department. In fact, in March we will be at our fifth anniversary. So I think this is a particularly good time to take stock of where we've been, what we've accomplished over the last year, what lessons we can draw from our experience, and to think about the challenges that lie ahead and how we are going to address them.

2007 was, in fact, a year of tremendous progress and maturation for this Department. From border security and immigration enforcement to passenger screening, critical infrastructure protection, and emergency response, we launched a number of important initiatives to strengthen our nation's security and we began to see the fruits of our labor in a number of vital areas.

The year was not without its challenges. While there were no successful terrorist attacks here in the homeland, we did continue to face serious threats, including plots against Fort Dix, N.J. and JFK Airport. These plots were disrupted by our partners and ourselves through sound intelligence, including, in one case, information provided by an alert citizen in N.J.; and all by working in partnership at the federal, state and local level, and with the private sector.

We're also fortunate that this year ended without any major hurricanes striking the United States, although there were a couple of major hurricanes in Central America. However,

we did suffer unprecedented wildfires in California, floods, drought, deadly tornados in several states, an ice storm that continues to impact on almost a million people who were without power in the Midwest. Indeed, the wildfires in California forced an estimated 320,000 people to leave their homes at one point, which I think is probably the largest evacuation we've had in the country since Hurricane Katrina.

We also saw record numbers of air travelers at our airports, including more than 17 million travelers during the week of Thanksgiving. Despite this high volume, and the continued and necessary restrictions on liquids in carry-on baggage, peak wait times at the busiest airports rarely exceeded 13 minutes -- and in most places, were substantially lower.

This, by the way, is a great non-story story. If there had been a lot of long lines and complaining passengers, I guarantee we would have seen a lot of news media attention. But there was comparatively little to the absence of complaining in long lines, and I think that's a tribute to our TSA screening work force.

But it also underscores one of the challenges of this department, which is that often, accomplishments are unsung because they're quiet accomplishments, because we've avoided a problem rather than because we've embraced a problem. And therefore there's an extra challenge on us to make sure the people at DHS understand how much we appreciate the work they do, which often is in what they avert from happening as opposed to something affirmative that occurs.

Now, 2007 was also a year in which we fought a tough battle in Congress on the issue of immigration reform. And I have to say candidly, we missed a critical opportunity, not through lack of effort but through lack of result, to implement a comprehensive solution to a decades-old problem that we know cannot simply be solved by enforcement. Unquestionably, enforcement is a critical element and a foundation to solving the problem, but it is not, at the end of the day, the complete solution.

Through all of these challenges I've outlined, the 208,000 men and women of the Department of Homeland Security continue to stand watch over our borders, our ports, our skies, and our homeland, and to keep their pledge to the American people never to lose their focus, never to grow weary or to grow complacent, and to do their level best to protect our nation. They deserve our gratitude for a job well done.

Now, I'm not going to tell you that we achieved perfection. No human effort is without error -- and we had our share of errors this year -- but we did learn, we matured, we challenged ourselves, and we grew stronger and more united as a department. And so, what I'm going to do in the next minutes is to take the opportunity to review some of our key accomplishments, particularly with regard to what I have often described as our five overarching goals.

What are these goals -- keeping dangerous people from entering the country; keeping dangerous goods from entering the county; protecting the critical infrastructure on which

our lives and our economy depend; strengthening emergency response and building a culture of preparedness; and finally, improving the department's management.

And then after I've reviewed where we are at the end of 2007, I'd like to talk about four issues that will demand our sustained attention in 2008 and likely beyond: immigration and border security; secure identification; cyber security; and the continuation of our efforts to institutionalize the department's functions; and more than that, to make sure this country is philosophically and mentally prepared for the challenges ahead, with respect to these threats that we face.

First, let me talk about protecting against dangerous people. What this really depends upon is having advance information about who's coming here, having the ability to quickly and accurately confirm the person's identity and to check him against watch lists, preventing the use of fraudulent documents, and determining who the unknown terrorist is; the terrorist whose name we haven't yet identified but who is nevertheless a real threat and someone that we ought to keep out.

Now this challenge is particularly remarkable when you consider that over the past year, more than 414 million people came through our ports of entry. That means we literally had seconds to determine the level of risk of each one of these people. And we had to determine that level in a way that allowed the vast majority of innocent travelers to pass without hindrance, while making sure we didn't commit errors that would admit a terrorist or a serious criminal.

We have made some very important strides to improve our ability to screen these travelers who come into the U.S. Earlier this year, we reached a landmark agreement with our European counterparts to continue sharing advance information on passengers arriving and departing our country. These are known as Passenger Name Records. And we did it in a way that was consistent with and strengthened privacy protections. This data, which is basically commercial data collected by the airlines that identifies things like your contact number and your credit card, has allowed us to identify scores of dangerous people and to keep them from entering our country. In fact, this system is now so successful that the European Union has proposed adopting it for itself.

Now as part of this effort, we've implemented a new rule that allows us to get Passenger Name Record information earlier from the airlines than we previously did. This allows us to conduct security checks before flights take off, and minimizes the unhappy circumstance where we discover someone's on a flight who's dangerous, and we have to turn the flight around. So that clearly is one way to help us identify people who are threats.

But another way is using biometrics -- physical characteristics, fingerprints. We have for some time taken two fingerprints, two index fingers, from people who either want visas to come into the U.S. or for people who travel without visas; for people who present themselves at the ports of entry. But in order to improve our ability to confirm identity and check visitors against watch lists, this year we began taking 10 fingerprints. More

than half of our consulates overseas now take all 10 fingerprints electronically as a precondition to giving a visa. And just this last week at Dulles Airport, we began the process of taking 10 fingerprints at our ports of entry in the U.S.

Why is it important? It's important not only because it's more accurate to have 10 fingerprints than two fingerprints, but because 10 fingerprints allow you to match the fingerprints of a traveler against the latent fingerprints -- that's the fingerprint residue -- that we collect all over the world at crime scenes, in safehouses where terrorists plan, even on battlefields. And I've actually seen a picture of the remains of a truck bomb in which latent fingerprints -- you can see the residue of the latent fingerprints on the door that had been lifted and categorized in a database.

Because of our capability to take 10 fingerprints, and the collection of latent fingerprints from battlefields and training camps and safehouses, we now have a much enhanced capability to identify the unknown terrorist; the person whose name we don't have on watch list, whose biographic information may not tip us off to the threat, but who has left a little piece of themselves somewhere and some place that suggests we ought to take a closer look.

This, by the way, is not only operationally significant, it's a magnificent deterrent, because now that we have made it clear that we will collect and use these latent fingerprints, any terrorist who has ever been in a safehouse, or a training camp, or built a bomb, is going to have to -- is going to have to ask themselves one question before they decide to come to the U.S.: Have I ever left a fingerprint anywhere in the world that has been lifted and captured and entered in a database? Because each of these terrorist trainees or bomb makers is going to know that if we have lifted their fingerprint and it is in a database, we will catch them when they cross the border -- and fingerprints do not lie.

The Coast Guard is also leveraging the power of biometrics. Working with U.S.-VISIT, they have launched a biometrics-at-sea program to capture fingerprints from individuals who are attempting to enter our country through the maritime domain, between Puerto Rico and the Dominican Republic. In its first 12 months, this program has reduced the flow of illegal migration in that area by almost 50 percent, and next year we're going to expand it to the Florida Straits.

But we're looking not only at previously identified threats, we're looking at new and emerging threats. We've proposed new rules to strengthen the security of general aviation aircraft, private aircraft, entering the United States. This complements the efforts I've described that are focused on commercial air travelers. After all, the last thing we want is for a terrorist or a terrorist weapon to slip into our country on a private aircraft or a charter jet. So this year, we began to require more comprehensive information about passengers and crew on those private aircrafts before they leave to travel to the U.S. And we're moving forward with new initiatives to conduct screening and inspection of private aircrafts overseas before they leave to arrive at our shores.

This, of course, is the use of all of these intelligence tools to identify dangerous people. But one of the most fundamental tools is identity. If we do have someone on a watch list, or we do know someone who's a criminal and shouldn't be admitted, then, of course, it's very important that we can ascertain they're not masquerading as somebody else.

And so to close a known vulnerability, one identified by the 9/11 Commission -- travel documents -- we have initiated the Western Hemisphere Travel Initiative. This was passed by Congress. It reflected the 9/11 Commissions's observation that in the hands of a terrorist, a forged or stolen document is like a weapon. And what it requires is that we have only robust and secure documentation acceptable as a form of identification to allow you to enter the United States.

As part of the Western Hemisphere Travel Initiative, this year we began requiring citizens of the U.S., Canada, Mexico and Bermuda to present a passport when arriving at our international airports. This closed a vulnerability that had existed, because people traveling from these locations with those citizenships had previously been allowed to appear with literally hundreds of different kinds of documents, which were very difficult to inspect and check for fraudulent nature or for their being counterfeit.

Because of the Western Hemisphere Travel Initiative, we have greater confidence that a person isn't using a phony document to enter the country. And here is the good news: the people get it. Compliance under this rule has been close to a hundred percent, which illustrates that we can in fact strengthen travel document security without damaging the flow of people that make our country both a welcome destination, and also help and improve our economy.

Now while I'm later going to discuss some of our illegal immigration-directed efforts a bit more, I do want to note that we have made considerable progress this year, protecting the the American people from dangerous people who have entered illegally: criminal aliens, fugitives and gang members.

This year we arrested more than 3,500 illegal alien gang members and their associates. ICE -- Immigration and Customs Enforcement -- added 23 new fugitive operations teams to identify and capture and deport illegal aliens who have defied a court order to leave the country. These teams arrested more than 30,000 fugitives -- nearly double the arrests in the prior fiscal year.

Now as I said, our mandate is not only to protect against dangerous people entering the country, but also dangerous goods, including, in particular, goods that might be radioactive, or other weapons of mass destruction.

Our approach here is not to rely on any single layer of protection, but multiple layers of protection. This reflects the common-sense observation that while human failure is inevitable in any system, the more systems you build with different kinds of capabilities, the less likely that that failure will persist throughout all of the individual gates that something or someone has to pass.

It's a little bit like if you've ever landed on an aircraft carrier, the tailhook has a number of different bands across the carrier deck that it can catch -- not just one, but several. And the idea is a recognition that the pilot will sometimes miss the first tailhook, and the tailhook will miss the first band, but it will hit the second one or the third one or the fourth one or the fifth one. And that principle of multiple layers, which works on aircraft carriers, also works in securing our borders with respect to dangerous things and dangerous people.

So this year, we launched our Secure Freight Initiative at six overseas ports. This is designed to test our ability to scan 100 percent of inbound cargo for radiation before the cargo was loaded on a ship to come to the United States. This is part of pushing our defenses and our security outward, and it's an effort we undertake in partnership with our allies and friends overseas.

As part of Secure Freight, we're also going to continue to require that we obtain more information about what is in cargo shipments, and collect more trade data from the private sector. This gives us better visibility into the supply chain, and a crisper ability to identify those kinds of shipments that we ought to take a closer look at. This is intelligence-based screening, and it's another layer, in addition to the overseas scanning, which helps us assure the security of our borders.

Complementing Secure Freight overseas, we also expanded our Container Security Initiative to 58 foreign ports. Here, again, using the tools I've described -- the scanning and the intelligence-derived information -- our inspectors now work with their foreign counterparts to screen cargo before it's loaded on to the ship. And with the current deployment, more than 85 percent of the containers shipped to the U.S. now transit through CSI ports and benefit from our overseas inspection.

With respect to our own ports of entry at our own border perimeter, we achieved a major milestone this year with the dependent of our 1000th Radiation Portal Monitor. Today we are scanning more than 97 percent of inbound cargo for radiation at our seaports -- over 90 percent at our northern border and 100 percent along our southern border. And next year, we will complete the job of getting pretty close to 100 percent at our northern border as well.

All of these layers make our maritime domain safer and our land domain safer, in terms of shipping in goods. But again, we want to make sure we're looking not only at the identified threats but the emerging threats and the threats that we haven't yet identified. And that means we have to look at not only large vessels and containers on trucks or on ships, but we have to look at small vessels. We know from experience that small vessels can be a vehicle for USS Cole-style attacks carried out by terrorists, and we also know from experience that small boats can be used to smuggle in dangerous things and dangerous people, including drugs.

And so we are working with the Coast Guard to begin to extend our capability to protect against the use of a small vessel to bring in radioactive material. We've got two programs now, one in Seattle and one in San Diego, that will use technology to scan small vessels entering those ports.

Additionally, as part of our effort to stem the flow of drugs, this year Coast Guard -- this past year Coast Guard seized 350,000 pounds of cocaine worth an estimated street value of $4.7 billion. That is a new record, and it is supplemented by additional enforcement successes through Customs and Border Patrol, ICE, and our Office of Counter Narcotics Enforcement.

Let me turn to the third element of what we have been accomplishing this year, and that is strengthening our domestic critical infrastructure. We used congressional authority that we received late in 2006 to implement tough, new chemical security regulations designed to protect chemical facilities from attack, and to prevent the theft of chemicals that could be used as weapons. As part of this effort, we work with the chemical industry to devise performance-based standards -- not standards that give us the ability to micro-manage private business and tell them how to do their business, but rather, standards that set metrics and requirements, hold them accountable to meet those metrics and requirements, but allow them to devise the particular way in which they can best achieve those metrics and requirements without sacrificing the core of their business.

We also accelerated our IED awareness campaign, boosted science and technology research into explosives, and expanded participation in our information-sharing portal to share expertise and raise awareness of the threat posed by IEDs.

At our seaports, we began enrolling port workers in our Transportation Worker Identification Credential program to protect our nations airports and air travelers. We proposed new regulations that will allow TSA to take over the control of domestic passenger watch lists under our Secure Flight program. This is a benefit to everybody in this room, because by far the largest reason for the errors that you experience when you travel by air, in terms of watch lists, are errors that occur because airlines have not properly inputted changes that we have made in the list to make the list more accurate. If we can take the management of this list on board to TSA and run it ourselves, we will not only be more accurate and more secure, but we will reduce the error rate.

But TSA, again, is another agency that is using this philosophy of layered defenses as a way of making sure that we don't compromise our security simply because human error means that any single defense is not perfect.

We not only have watch lists, we not only have the TSA screening function, but we are now deploying behavioral screening officers to more than 40 of our nation's airports in order to identify potentially threatening passengers based on their behavior. We've learned lessons, for example, from the Israelis and the Europeans in how to train our screeners to look for certain kinds of behavior that denotes a possible threat or an uneasiness that warrants a closer inspection. This is a proven tool. It enhances yet

another layer of security, and it helps us build an element of randomness in the process, which is very important in terms of deterring terrorists.

Both of these programs reflect our determination to move beyond the static, inflexible model of checkpoint screening, with which we began TSA, to a more dynamic and multi-layered security environment that includes, apart from behavioral detection, such tools as whole body imaging, and a focus on improvised explosive devices. We'll be expanding this concept next year because it's not enough to simply say we've avoided another hijacking on our aircraft since September 11th. We have to make sure we keep ahead of the enemy so we can continue to avoid those kinds of hijackings.

To protect our nation against biological threats, another big concern in terms of weapons of mass destruction, our Office of Health Affairs, which we created this year, thanks to congressional authorization and appropriation, established the National Biosurveillance Integration Center to provide common awareness and early detection capability of biological events and trends. To promote information sharing and help combat homegrown terrorism, we increased our participation in state and local intelligence fusion centers, deploying additional analysts and further distributing our Homeland Security Data Network, the secure information-sharing portal.

Our Office of Intelligence and Analysis works with the Office of Civil Rights and Civil Liberties to study the threat of radicalization in our country, and we did a good deal of outreach to the nation's Arab and Muslim communities. And we reached out as well to the business community, completing the sector-specific plans of our National Infrastructure Protection Program that sets security priorities, defines roles and responsibilities, and boosts partnerships between the public and the private sector across all 17 infrastructure areas.

Now let me turn to emergency response. As I've said, we are an all-hazards department, and heaven knows we've seen just about every kind of hazard you can see over the past few years. This year, as part of an effort since Hurricane Katrina to retool and transform FEMA, we had the opportunity to test some of the developments in FEMA that we have put into place over the last 24 months, including better tracking of commodities, pre-arranged mission assignments with the Department of Defense that allow us to move more quickly to deploy Defense Department resources, and improved disaster registration.

From the standpoint of personnel, for the first time in recent memory, FEMA has permanently filled all 10 of its regional director positions and 95 percent of its full-time positions -- basically full employment. We've also restructured FEMA, giving it new directorates and a new organizational structure.

FEMA's employees are finally getting the tools and capabilities they have lacked for decades. As a result, FEMA's response time improved over the past year, and FEMA was praised for being on the scene quickly during the California fires, the tornadoes in Alabama and Kansas, and other disasters. And to make sure that state and local officials

have the ability to communicate during a disaster, this year we awarded $1 billion in Public Safety Interoperable Communications grants and released interoperability scorecards for 75 urban areas in our country.

With all of this, the last area of accomplishment is in the integration and unification of this department. It's a young department, it's not even five years old, and we have to continue to work to integrate the core management functions and to achieve a cohesive and unified agency.

Part of what we're doing is unifying our information technology services; creating a robust and multi-disciplinary training and education template for our employees; advancing our plans, with Congress's help, I hope, to move the department's headquarters to St. Elizabeth so we can actually join everybody in the same physical space; unifying information technology budgets under our Chief Information Officer; and of course trying to foster career development and a happy workplace for the 208,000 men and women of this Department.

So that's what we've done over the last year, but we've got a lot left to do, and I've got four things in particular I'd like to talk about for the year to come.

First, border security and immigration. I don't think there's an issue on the domestic front that has been more emotional and of greater public concern during my lifetime, except perhaps for the civil rights revolution in the 1960s, than the issue of illegal immigration. There's profound public skepticism about the government's willingness and ability to control illegal immigration.

I said it at the beginning of the speech and I'll say it again: In the end, the most efficient and the most humane way to deal with this problem is to deal with it comprehensively. But I recognize that the government needs to make a down payment on credibility with the American people by showing we have the willingness to enforce the laws the way they are, and that we're prepared to use all the tools at our disposal to get the job done. And that's a good deal of what we've done over the last year and what we intend to do over the year to come, although I am not prepared to give up on some kind of comprehensive reform, or at least some progress toward comprehensive reform, during 2008.

This past year, we added more than 87 miles of new pedestrian fence and 61 miles of vehicle fence along the Southwest border. We now have 165 miles of pedestrian fence and 118 miles of vehicle fence between the Pacific Ocean and Brownsville, Texas. That's a grand total of almost 300 miles.

Next year, we're going to continue to install more than 200 miles of pedestrian fence and 180 more miles of vehicle fence to bring us to a total of 670 miles of fencing, pedestrian and vehicle. That's basically going to give us the ability to put some kind of a barrier in place, from the Pacific Ocean to the New Mexico-Texas border, except in those areas where there's a natural barrier. And we will also be putting some fencing in Texas as

well. But again, I have to say, our ability to complete the mission, which we have planned and which we are prepared to do, depends upon Congress giving us timely appropriations that lets us get the job done.

We increased our Border Patrol staffing by 21 percent, from 12,349 agents to, in fiscal year 2006, to what will be 15,000 agents at the end of this calendar year. This is the largest yearly increase in the history of the Border Patrol. And we are well on the way to the promise of doubling the size of the Border Patrol under President Bush, since next year we will have over 18,000 Border Patrol agents.

Now, these men and women need effective tools. We've added new technology at the border, ground-based radar, unmanned aerial systems. And this month we conditionally accepted the first stage of our virtual fence under SBInet.

A fair question: Has our effort had an impact? Well, apprehensions at the border were down over 20 percent for fiscal year 2007. When you combine this with other indicators, this reflects the fact that fewer people are attempting to cross, and that our strategy is beginning to work.

Part of the strategy is also increased interior enforcement. ICE had a record year -- more than 850 criminal arrests in worksite enforcement cases for 2007, exceeding last year's record total. And we expanded programs of training state and local law enforcement officials in 30 agencies to help us do our job.

We also expanded tools to help employers check when their employees are authorized to work in this country, and participation in our electronic e-Verify system more than doubled over the past year.

But I have to say, we're beginning to hit some heavy weather. I am sometimes asked why it is that for 30 years we seem to have trouble in the United States enforcing the rules against illegal immigration. And I'll tell you what the answer is. The answer is that when the television cameras turn off and the spotlight moves to something else, there are a host of interest groups and advocacy groups who work very, very hard to make it difficult to enforce these rules. I'm not commenting adversely on their motivation, but I can tell you the effect of all of this is to wear down the ability of an agency to enforce the law.

We tried to put into effect a regulation to help employers clear up instances where a worker's name and Social Security number don't match. Quite candidly, some members in the business community explained why they objected to that regulation, because in some parts of the economy, most of the workers are illegal, and they were afraid if we enforced the law, that would hurt their business. I sympathize. I think there's a right way to address that concern by making changes in the law to address the labor need. But I also know there's a wrong way to address that concern, and the wrong way is to shut our eyes to law-breaking and create what I call a silent amnesty, and we will not do that.

And so we are in court, working to make sure that we can get this regulation freed up to enforce this coming year. In some cases, we've actually had to go to court ourselves in order to deal with impediments to enforcement. We currently have a lawsuit against the state of Illinois seeking to strike down legislation that the state put into effect that actually would have made it virtually impossible for employers on a voluntary basis to subscribe to our e-Verify program. We don't necessarily require that states and localities enlist in helping us do our job enforcing the law, but we sure are going to tell them, don't stand in our way when we try to do our job.

As Chairman Hamilton knows, one of our best defenses against terrorism is secure identification, and that's the next big item I have for 2008. And again, to repeat the words of the Commission, "sources of identification are the last opportunity to ensure people are who they say they are and to check whether they are terrorists." We continue to face a real vulnerability in this country due to the lack of secure identification. We need to bring identity document standards into the 21st century to protect terrorists and criminals from using fraudulent ID, and to prevent against identity theft.

And so we're moving forward on three fronts to create a robust, real set of security standards on which the American public can rely. The first of these is Western Hemisphere Travel Initiative, which is designed to assure that when people come into this country, they will have a form of identification that is not easily fabricated or counterfeited, and on which we can rely.

Starting in 2008, we will begin moving to a WHTI-compliant land-crossing rule, one which I think we can implement with a minimum of pain, but one which is indispensable if we're to move from the current system, in which people present 8,000 different kinds of identification to cross our land borders, into a system where we can reasonably rely on the documentation presented, so that the border inspectors can do their jobs.

A second element of what we're trying to do is the Enhanced Driver's License. This is designed, actually, to be a win-win for security and convenience. We've invited a number of states and provinces in Canada to work with us to convert their driver's licenses into the kinds of documents that will satisfy our Western Hemisphere Travel requirements. This will not only create a less expensive means for regular cross-border travelers to cross the border without having to get a passport, but will enhance the security of those licenses so that we can rely upon them again as a security measure.

And finally we are moving forward with a retooled REAL ID requirement, which we expect to put out in public form through new regulations in the very near future. Again, REAL ID was another 9/11 Commission recommendation that recognized that, like it or not, driver's licenses are still relied upon in most places as a principal means of identification, and that the current patchwork of rules and standards are inconsistent, and therefore make it very easy for somebody to game the system, phony up a driver's license, and then exploit that to commit a crime or an act of terror.

Although we have paid close attention to the concerns articulated by a number of states about REAL ID, and although I think the regulation we are going to be issuing within a matter of weeks will do a lot to satisfy some of these concerns about cost, I have to recognize that some people have an ideological discomfort with having REAL ID driver's licenses.

I think we ought to have this debate. I have yet to hear a persuasive argument for why it is a good thing for privacy to have driver's licenses that are easily forged or counterfeited. I have yet to have anybody explain to me why I'm better off as a citizen if a 16-year-old kid in a college town can take my identify, phony up a driver's license, and pretend to be me. It seems to me that driver's licenses which are secure, which are issued on a basis that has appropriate underlying documents, and which cannot be counterfeited, is not only good for security, but it's good for privacy for every American citizen who wants to be able to safeguard their own identity against identity thieves.

Third area that's on our agenda for next year is cyber security. This is an area, of course, of virtual reality, and as we enter the 21st century, we're acutely aware of the fact that much of our economic well-being as a country depends on our ability to use the internet and to use data systems in order to perform our work. We've created a National Cyber Security Division to help lead an interagency effort to strengthen cyber security. We've established the United States Computer Emergency Readiness Team to provide a 24-hour watch, warning and response center, and this year they issued over 200 actionable cyber alerts and notices on vulnerabilities and incidents.

We're also developing and expanding the capability of the Einstein Program, which detects malicious patterns in computer network traffic. And we are working with Congress, as we speak, on an enhanced cyber security strategy, which I believe will set the template for the next decade on how we deal with this emerging and increasing threat.

Finally I would like to talk about the need to finish the work of this department in a fourth area, and that is institutionalizing its operations and the homeland security mission. The fact that we have not had a terrorist attack on this country -- in this country in the last six years is not a cause for complacency or a time to celebrate the end of the struggle. The threat is not going away. The enemy has not lost interest. And if you had doubt about it, look at yesterday's reports about bombings in Algeria.

Fundamentally, we're in a struggle about ideology. Terrorists want to remake the world in their own image, and it’s an image that is intolerant of the kinds of institutions that we cherish. Again, is it an accident that the terrorists in Algeria chose to blow up a court and the United Nations Development Agency? It seems to me what they struck against was the rule of law and efforts to bring development and food and peaceful activity to people who need help in North Africa.

So our goal has to be to frustrate the aim of these terrorists and these ideologues. And from the standpoint of the Department of Homeland Security, it's important that we play our role in that joint effort by continuing to persist in our efforts to secure the homeland

and to stay ahead of the enemy, and to do so as a single unified institution that delivers on the promise that Congress had in mind when they stood up this department in the first place.

I'm pleased to say that in our short history, we've begun to see some of the benefits of institutionalizing our capabilities. Through TSA's Viper teams, we have brought together federal air marshals, transportation security officers and canine teams to conduct security measures in our ports and transit stations. Through the Coast Guard's Deployable Operations Group, we've created multi-agency rapid-response teams that work together during emergencies and heightened-threat periods to boost security.

Our Border Enforcement Security Task Forces bring together Border Patrol and ICE agents, as well as state and local law enforcement, to fight crime at the border and prevent the entry of contraband. Over the past year, for example, these BEST task forces made more than 500 criminal arrests, and in June a BEST team arrested one of Mexico's ten most wanted, who had been a fugitive since 2002.

So we've done a lot to institutionalize our agencies and functions, but I have to be candid in saying we still face some obstacles this year, and one of them has to do with congressional oversight.

Once again, let me go back to the 9/11 Commission Report. The 9/11 Commission challenged Congress to streamline its oversight of the department. Much to my dismay, this recommendation on streamlining oversight has gone largely unheeded. We have a strong relationship with Congress. We appreciate the need of oversight. We have good relations with our oversight committees and our appropriations committees. Good oversight actually helps us do our job better and ensures we get the resources we need. But because Congress hasn't focused this oversight, we face a situation that I would describe as oversight run amok.

Our department reports to 86 congressional committees. Over the last year my colleagues and I have been called to testify 224 times; that averages to about four times a week. Since the department's creation, DHS officials have testified 761 times, provided roughly 7,800 written reports and answered more than 13,000 questions for the record.

Obviously this is a drain on the department's time and resources, but honestly I wouldn't be up here talking about this if that was the only problem. There's a more serious problem at hand. Because 86 committees and subcommittees hold some level of jurisdiction over the department, these committees tend to look at us through the prism of their own particular, specific interests. They don't look at the big picture in terms of what's best for nation's security overall, and how do we best make these trade-offs.

Our country needs to have an honest discussion about the trade-offs involved in homeland security. You cannot make everything a priority. Spending decisions have to be made based on what's risk-appropriate and what is most cost-effective, and that means some things have to take precedence over other things.

Our main authorizing appropriating committees have the responsibility and the jurisdiction to work with us to assess and analyze those trade-offs, but when you have 80 or so other committees, each of which has a narrow slice of jurisdiction that also seeks to have input into how we prioritize and how we make trade-offs, then you have a recipe for conflicting direction and constant fighting about who controls jurisdiction over what part of my agency. This, to be honest, is part of the reason we have seen a lot of organizational churn at DHS over the last year. Every committee feels it wants to put its own imprint on the department.

My plead stays for Congress to streamline its oversight. We welcome the oversight that the authorizing committees have and the appropriating committee has -- committees have, but please give us a reasonable number of points of contact so that we can engage in a dialogue with Congress in a way that is disciplined and allows us to pursue in a joint fashion the kind of overall assessment of what is important and how to manage this department; that only those who have the big picture have the ability and the incentive to pursue.

I'd like to close by asking what may be, in my mind, the most fundamental question for the year that we're about to enter. Why are we doing all of this? Why are we taking all the steps that I've described to protect this country? Well, on a personal level, for me the answer is very simple. When I became Secretary, and the reason I became Secretary, was to make a commitment to do everything in my power and within the bounds of the law to prevent another terrorist attack against our country.

Like almost everybody in this room, I was in Washington on September 11th. I knew people who perished in the attacks of September 11th. I've met with family members who lost loved ones at the hands of terrorists, and have asked me the question, how could this happen? Can you promise us it's not going to happen again? And I've talked with first responders who have had a colleague who didn't return home on that day. I am acutely aware of the responsibility that rests upon all of our national leaders, in all branches of government, to make sure that we do not lose innocent lives in this struggle against an implacable and remorseless enemy.

Now when I hear people say the terrorist threat has diminished, or maybe we don't need to take it so seriously, or they're concerned that security is going to be inconvenient or it's going to cost too much, I have to say, these excuses will ring hollow if we're attacked again and if we haven't done everything reasonably necessary to prevent that attack, protect against that attack or respond to the consequences. That doesn't mean absolute security at the cost of everything, but it does mean a clear-eyed and a hard-thinking look at what the trade-offs ought to be to manage the risk, and a willingness to spend the money that's necessary to give us a reasonable assurance against a risk that if it comes to pass might have catastrophic consequences.

I believe this department, I believe the U.S. government as a whole, I believe our allies have a better set of capabilities and tools now than they've ever had to deal with this

threat. But I think the most important ingredient we have to have as we move forward next year and in the next five years and the next 10 years is the proper mind-set. We have to have a resolve and a determination to continue to be vigilant and to stay ahead of the enemy if we are going to continue the record of repelling attacks since September 11th.

As I enter my last year as Secretary, I can tell you I will give it my all, and it is my promise and my intent to turn over to my successor, when a new administration comes along, a department that has fulfilled the promise and is a mature agency -- with more work to do, but a firm foundation on which to build.

That's why we're going to drive to complete many of the efforts I've discussed today. We obviously will continue to listen and learn and grow as a department. We're going to work with Congress, and in a spirit of collaboration with our state and local partners and with the American people, because all of us have not only in an official capacity, but in a very personal capacity, a stake in the success of this department, and a stake in the success of homeland security.

So I'd like to thank you for your support, and I would like to wish all of you a safe and happy holiday season. God bless you. (Applause.)

###