

## Remarks by Secretary Chertoff to the International Association of Chiefs of Police



Release Date: November 11, 2008

San Diego, California  
International Association of Chiefs of Police

**Secretary Chertoff:** Thank you for that very warm welcome. I want to make note of the fact that this is, of course, Veterans Day. I had the privilege a few moments ago, to swear in about 135 new American citizen sailors and marines from 37 different countries and it was a heartwarming experience to bring new citizens into the fold who have served their country even before they had the full rights to citizenship. It is also I know the day after the birthday of the Marine Corps, so happy birthday to all of you Marines out there.

I knew that would be an applause line.

I am delighted to be here again with the IACP, and again, to be able to talk to you a little bit about our common interests and our common goals; and also to thank you for the support you have lent to our efforts to secure our country against terrorism and other kinds of global threats, whether it be transnational criminal activities, mixed terrorism and narcotics trafficking; whether it be terrorism from the Al Qaeda networks, or terrorism from other networks, you have been partners of ours and that is a partnership which needs to continue and which I am convinced will continue into the next administration.

We, of course, want to continue to work the strength in that partnership, which for that reason, we have created an office for state and local law enforcement led by someone I know you know very well, Sheriff Ted Sexton. His job, which he performs very well, is to make sure that I have a direct line of communication to the law enforcement community, and that you have a direct line of communication with us. And because he has a three-year appointment, I anticipate that Ted will continue to be that direct line of communication to my successor as Secretary of Homeland Security after January 20th.

Our partnership is also the reason we've worked hard over the last five years to identify ways to meet the needs of police officers across the country who are working on the front lines to protect our communities from acts of terrorism and other threats to the American people. I would like to take a few minutes today to talk about some of the areas of collaboration and cooperation that we have achieved and, in particular, discuss two areas where we are continuing to focus on improving our capabilities and releasing our vulnerabilities.

The first of these efforts is sharing information about suspicious activities, whether it protects at the federal, state, or local level. This is what we call suspicious activity reporting. The secondary effort concerns the growing problem of identity theft. As you know, identity theft is a favored and increasing tool of criminals who seek to conceal their identities in order to commit crimes. It is also a way for people who are not authorized to work in this country to get work illegally, and often cause an enormous heartache to the people who are the real owners of the identities that have been stolen.

But before I talk about these two issues, I would like to note a few recent adjustments that we've made to some of our existing programs in response, frankly, to the feedback we have gotten from the IACP and others in the law enforcement community.

The first of these areas is an issue of grants. As you know, last week we announced our fiscal year 2009 grant guidance. We will be awarding \$3 billion in total grants for a host of activities including planning, training and exercises, prevention of the detonation of improvised explosive devices, information sharing, medical readiness, and radiological and nuclear detection.

Since 2002, we've made available \$27 billion in grants to our state and local partners including our law enforcement partners. As in the past, this year we will continue to focus on a risk-based priority and building national critical capabilities. In addition, we will be providing more flexibility on how some of these grant funds can be used. Specifically, we will be removing restrictions on personnel costs under the Homeland Security Grant Program, including allowable personnel expenses up to 50 percent, and also removing the 3-year funding limit for intelligence analysts. I know that was an issue that I heard a great deal about over the last year. I believe is

going to give law enforcement agencies greater flexibility to cover the costs that are associated with those activities that are focused on counter-terrorism.

For 2009 we've also strengthened the position of law enforcement terrorism prevention activities by ensuring that there are a separate set of priorities for that stream of funding. We also included a specific dollar amount required to be spent on law enforcement terrorism prevention activities. The result has been a significant increase in funding available to law enforcement over the last two grant cycles from \$363 million in 2007, to \$429 million this last fiscal year, and \$434 million for the upcoming 2009 fiscal year.

In a separate area let me briefly mention we're going to be making some changes to our procedures for law enforcement officers who fly armed. As you know, we have a set of requirements for officers who fly armed on commercial aircraft with their weapons. That includes carrying a letter of authority confirming the need to travel armed and detailing your itinerary. We are taking a look at a way to streamline and improve this program, including a more standardized system for tracking officers who fly armed are in a better identification verification system.

In the short term, we are going to transition to a national law enforcement telecommunications system, or NLETS message for state and local law enforcement officers flying armed. This message, sent by your employing agency, will be in addition to the current letter of authority that is now required. In essence it means that officers will need to send their travel data to TSA via the NLETS system, and then they will receive a unique alphanumeric code for verification at the airport on the day of travel. This process will begin on November 15th and other procedures will continue to remain the same.

Now let me talk about the two initiatives I mentioned earlier, first, beginning with information sharing and suspicious activity reporting. We know one of the great lessons of 9/11 was the need to connect the dots. And, of course, some of those dots are collected overseas and then we have to connect them here at home, but a lot of the dots are connected on the streets and roads of our American cities and towns. And it's important to make sure that in order to connect the dots, we can collect them in the first place. And that means we have to increase the way in which we are able to interact with our state and local law enforcement authorities to make sure we have top to bottom visibility into what might be suspicious activities.

Part of this effort has been the creation of our fusion centers at the state and local level. By the end of this year, we'll have 35 DHS analysts support the fusion centers around the United States working side-by-side with their state and local partners. And by the way, this is one of the reasons we are very interested in removing that limitation on funding for state and local analysts, so that we can really build up that set of relationships that, I think, will continue to invigorate the fusion center concept. It is our plan, eventually, to deploy up to 70 agents -- 70 intelligence officers and analysts -- including ones at each state-designated fusion center.

But another way to take this sharing to the next level is through suspicious activity reporting, which I know originated in California here through an initiative undertaken in Los Angeles. As you know, these reports are generated at all levels of law enforcement and contain law enforcement information that include potential connections to terrorism. We need to make sure that as we organically grow this system, we have a coordinated, standardized way to gather, analyze, and disseminate the fruits of the work that we are collecting at all levels of government.

And so the Federal Government, whose program manager for the information sharing environment, have begun a national suspicious activity reporting initiative so that we can have a set of shared databases that allow all law enforcement to network on a national level. This is not meant to be a top down process. It is meant to facilitate a bottom up network process.

And in order to make sure we can be compatible in the way we collect, format, and exchange this information, we are working through our initiative to develop a process to make sure we have common visibility, to get the reports through fusion centers, and then to be able to exchange regional and national analyses among our partners.

We're also testing a searchable library that would allow our partners to access the information on summary SAR reports through a web-based portal and, of course, an effort is underway to work with you to develop a best practices study to help identify best practices to report this information.

DHS is willing and happy to host this program if there is collective support for this initiative. That means, though, it has to be something that you all agree you want to do. And we believe that if we're going to do this shared initiative, it should have some core principals.

First, it needs to be built from inside your agency and it has to have the support of law enforcement at a state and local level, not just at a federal level.

Second, we need to have a common language, a common code. That's how we create a searchable -- a set of shared databases that we can exchange and use in a way that is practical and efficient.

And finally, we have to be organic in the way that this process moves. It has to be driven by a collaborative approach, as opposed to a mandatory approach. And, of course, one of these we want to do, at DHS, is to look to supplementing what you are putting into the system with input from our Federal Air Marshal Service and Coast Guard. So we look forward to working on this with you in the months and years to come.

The second major initiative I'd like to talk about for a couple of moments is information sharing on the issues of identify theft. We know identity theft is one of the fastest growing crimes in this country. Because more and more a person's assets, their livelihood, even their reputation may depend on the sanctity and security of their identity. And so in order to try to take our ability to exchange information and protect identity to the next level, I'm pleased to announce a new program at the Department that will fight identify theft at the workplace and bring relief to victims of crime, and the answer is a new act that we call Job Lock.

What Job Lock will do is allow victims of identify theft to, essentially, lock up their social security number so an identity thief cannot use it to get a job and, perhaps, to damage somebody's reputation and credit rating. Job Lock will build upon our existing program, E-Verify, which is an automated, web-based system that allows employers to check to make sure that a newly hired employee is eligible to work in the United States. Currently, one of eight new hires in the U.S. is checked through E-Verify on a voluntary basis and this number of companies that use E-Verify has literally grown by about 1,000 a week.

If we add Job Lock to E-Verify we're going to take some of the profit out of identity theft. And remember, last year we estimate that over 8.5 million Americans were victimized by identity theft. In fact, the FTC tells us that the third most popular use of stolen identities is to get a job, so if we are able to use Job Lock to make it difficult for identity thieves to get jobs with stolen identities, we are going to put a major crimp in the network of identity thievery, which is growing in this country.

But we are going to need your help to make it a success. In order to make sure that Job Lock is not abused, our proposal is to lock the names and social security numbers of identity theft victims only if we can verify that they are truly victims of identity theft, and that means that anybody who wanted to join Job Lock must submit a police report and file a complaint with the FTC's consumer sentinel database. That will give us the ability to make sure people don't try to use Job Lock to make mischief of people that they're trying to injure in some way.

Many police departments already focus on fighting identity theft, but in order to make Job Lock work, we hope you'll all cooperate by encouraging your departments to take reports of identity theft and file criminal reports and police reports, which the victims can use in order to lock up their identity on Job Lock.

We going to need your help to make sure that people -- police officers do take these reports, and that the report number is posted with the victim's FTC consumer sentinel complaint. I hope you'll assist in getting the word out on Job Lock. I think it is going to make your jobs easier, it's going to help us protect victims of identity theft, and it's going to turn technology into a tool that enables us to protect victims of identity theft as opposed to a tool that's been used to harm people with identity theft.

Let me conclude by saying that as we navigate the upcoming Presidential transition, I want to assure you that you will continue to be a central part of the Department. I will personally assure when talking to my successor that I emphasize the importance of the partnership with law enforcement as the very core of what the Department of Homeland Security does; and I am also going to ask you for your support.

We know that a period of transition is a period where there may be some increased vulnerability to a terrorist attack. There may be the perception that we are being distracted, or there may be a sense that there is an opportunity to exploit new people who have come into positions of leadership at the Department in order to carry out some kind of a terrorist attack.

We are going to do our part -- everything possible -- to prepare and to exercise with the new people to get them as ready as they possibly can be to assume a leadership role, but we also know that the continuity of protecting this country lies with you who have been on the job since we were here, first created in 2003, and will continue on the job through the next administration.

So we want to make sure you are full partners in this transition and our commitment is to work to make sure that you have a seamless relationship with the new team that comes into DHS. And the last thing I'll say, it comes down to vigilance and commitment. I know we can count on you to continue to keep our country safe.

Thank you again for inviting me to be here today. We are grateful for your partnership and your support. Thank you very much.

###

This page was last reviewed/modified on November 11, 2008.