



## Press Room

- [Press Releases](#)
- [Speeches and Statements](#)
- [Testimony](#)
- [Multimedia](#)
- [Contacts](#)
- [En Español](#)



The threat level in the airline sector is **High** or Orange. [Read more.](#)



## Remarks by Homeland Security Secretary Michael Chertoff at University of Southern California National Center for Risk and Economic Analysis of Terrorism Events



Release Date: August 13, 2008

Los Angeles

University of Southern California National Center for Risk and Economic Analysis of Terrorism Events

**Secretary Chertoff:** I want to thank the Provost for that very kind introduction and even more so for inviting me to return again to USC to speak on the issue of homeland security and also to talk to some of the members of the first DHS center of excellence which I think is approaching, maybe it's already reached, its fifth anniversary.

As we're looking at our fifth anniversary at the Department of Homeland Security, which we celebrated in March, and as we look ahead to a change in the Administration, what I'm trying to do is to both look back and look forward in terms of some of the strategic lessons that we've learned and some of the strategic goals that we have to set for ourselves as we move forward to deal with the issue of homeland security in the very broadest sense of the word and so I'm giving a series of speeches over this period of time outlining the progress we've made and the challenges we continue to face in the area of homeland security.

The first speech, which I gave at Yale, dealt with the issue of the kinds of threats that are likely to bedevil us over the next 10 years, natural disasters like hurricanes and manmade disasters and attacks, like those launched by Al-Qaeda or other terrorist organizations or even the possibility of transnational organized groups, becoming a threat on a scale of a national security problem.

The second speech I gave at Rice dealt with the issue of our strategy of prevention. How do we prevent the manmade threats at least from being successful, from being carried out against citizens here in the United States, and how do we prevent dangerous people and dangerous things from coming into the United States where they might choose to launch those attacks?

Now, of course, there's other elements, there are other elements to our strategy. We have to talk about how we reduce our vulnerability if in fact dangerous people do come into the United States or if some of our own citizens become what's often described as "home-grown" terrorists and decide to carry out attacks against our institutions.

That's the issue of protection, and then my final speech will deal with the issue of response. How do we mitigate bad things when they happen?

But today's speech, which really focuses on the issue of protection, deals with one particular, I would argue, special challenge that we face on the eve of the 21st Century and it's a challenge that lies at the core of a great deal of what we do in protecting homeland security. It also lies at the core of a great deal of what we do protecting our financial security, our personal security, and our reputational security, and what I'm referring to is how we manage and protect our personal identities because I'm going to submit to you that in the 21st Century, the most important asset that we have to protect as individuals and as part of our nation is the control of our identity, who we are, how we identify ourselves, whether other people are permitted to masquerade and pretend to be us, and thereby damage our livelihood, damage our assets, damage our reputation, damage our standing in our community.

Now, often when we talk about the issue of identification, certainly over the last few years, it has come up in a very specific context. We talk about using identification to screen out dangerous or ineligible people from entering the United States through our borders, through our airports and our seaports, or from getting on airplanes or walking into federal buildings.

The 9/11 Commission spent a good deal of its time in the review of the events leading to 9/11 addressing the question of vulnerability and weakness in our identity security systems, the ease with which people could fabricate identities and use it as a way to live amongst us without being detected by the authorities or use it as a way to get on airplanes without being intercepted as somebody on a watch list.

But I'd suggest to you that identity is at the heart of a number of other very significant elements of our social fabric, even beyond simply protecting ourselves from terrorists or people who want to do us harm.

As we know from a lot of the debate over the last few years, identification is at the heart of the debate about illegal employment, people who come into the United States illegally and work illegally, and the question is how do we ascertain whether the people who are working for us are who they say they are so we can check their background, whether they are entitled to work so we can determine that we are complying with the law, and whether they are connected to the name in various tax databases so we can make sure that when we, for example, withhold the payroll tax, it's actually going to the right person?

So when you think about it, identity lies at the heart of the issue of employment which touches virtually every American. Identity, more and more particularly with the use of the Internet for purposes of transacting business, lies at the heart of our entire financial and market system. If we don't know who you are, if we don't know whether you are accurately representing your assets and your intentions over the Internet or even transacting business face to face, we introduce an element of risk into that business model.

The Internet depends upon the ability to believe that when you sell something to someone, that person in fact is going to be responsible to pay you and has the means to do it. When you get access to certain sites, when you withhold access to certain sites, when you safeguard information in certain databases, the key to entry and exit is again dependent upon identity. Are you a person who is authorized to get into that database, to remove that information, to see what's in there?

So when you think about it from that standpoint, the entirety of our economic livelihood in the 21st Century is going to turn in large measure upon our ability to verify identity for those who want to transact business, and, finally, our reputation and our privacy depends on our ability to control our identity. If people can pretend to be us, if they can speak in our name in an unauthorized way, they can do great, perhaps irreversible, damage to our privacy or to our reputation and this again from a personal standpoint suggests that identity is increasingly going to become the asset that we have to be most careful to protect in the 21st Century where the ability to get information, move it around the world and store it indefinitely creates greater and greater risks to personal reputation and personal privacy.

Now when I talk about identification, I want to separate two distinct elements because they are related but they are still separate. One is, we need to identify an individual as a distinct individual, a distinct person with certain rights and privileges. For example, everybody has a unique DNA and if we can identify that person and their DNA and know, for example, that

they are lawful citizens of the United States, certain consequences flow from that. You can vote. You can sit on a jury. You have the right to work and therefore we need to verify at a whole host -- in a whole host of circumstances that the person who presents himself or herself to claim a right or a privilege in fact is entitled to that.

But once you've made that determination, the issue of convenience and efficiency comes into play. How do we know in casual encounters and Internet encounters, at the airport or at the border, that you are the person who has previously been validated as having certain rights and privileges, and that's the issue of authentication.

So first we validate you. We determine in some form or fashion that you are a citizen, you are who you say you are, you have certain rights and privileges, and then we need a means that other people can test that validation, can authenticate that validation.

Now, before I talk about the different ways we do this, let me give you some concrete examples of how even in the last few years, we have increasingly seen a decrease in our ability to authenticate identity with very serious consequences for people all across the country.

Of course, the most obvious example is a situation of people who try to sneak in in order to do harm, terrorists, for example like the hijackers on 9/11, some of whom used false identification as a way to conceal themselves from the authorities or investigators so they could get on the airplanes that caused the tragic events of September 11th, and we've talked a great deal about the need to prevent people from exploiting weaknesses in our identity system in order to be able to get on airplanes and blow them up or enter places that they're not supposed to be and cause damage.

But there are also increasingly financial and other costs being borne by citizens apart from terrorism because we have not brought our identification management systems into the 21st Century. Some of these costs are not obvious to individual citizens. For example, credit cards routinely absorb fraud-related charges as "acceptable" losses. You don't necessarily know as a cardholder that that loss has been incurred. Oftentimes, you won't even be notified about the fact that they've somehow suppressed an effort to use your name in order to falsely acquire goods.

But the fact is everybody pays for this. Everybody pays for it in increased charge costs, in increased transaction costs, and in increased retail costs. So that's a widely-distributed but very real consequence of the imperfections we have in safeguarding identity.

Sometimes, though, these types of crimes or these types of exploitation of vulnerability in identity do hit the public radar. Last week was a good example. I was up in Silicon Valley and I announced what I think is the largest prosecution of identity theft in American history, an identity theft that took place over a period of years, according to the allegations in the indictment, which led to charges against 11 individuals, a scheme that is alleged to have involved the theft and sale of more than 40 million credit and debit card numbers hacked from eight major U.S. retailers.

This was truly, according to the allegations, an identity theft on a grand scale with the potential to generate millions of dollars of losses, based on people using these credit card numbers which are, after all, identifiers. They're the way you identify or validate someone's identity, using these credit card numbers to cash out at ATMs all over the place and to use these -- exploit these identities in other ways.

But apart from just the issue of the credit card industry and other financial services industries which increasingly suffer from identity theft, individuals suffer sometimes from identity thefts that occur on a very small level. Again, there's been a lot of discussion in the last year or two about the issue of people who are in the country illegally and working illegally. Some of them, of course, work without papers. Some of them simply make up papers out of whole cloth. They make up phony social security numbers and we try to tackle that using an electronic online system that you can use to check whether the name and the number are valid and matching, but increasingly, as we raise the bar to the simple schemes of impersonating legitimacy or legality, more and more of these people working illegally are using genuine identities that have been stolen from real people. In other words, identity theft has become a major enabler of illegal working in our economy.

Now some people dismiss this as an insignificant threat or an excusable effort on the part of people who are looking to work to evade the laws, but for those who believe it's a victimless crime, let me direct your attention to a *Wall Street Journal* article which I happened to read on August 7th of this year. It involved an individual from this part of the country whose name I won't use who discovered one day in mid 2003 that they had a letter from the IRS concerning \$18,000 in unreported income.

This person, however, had never worked in the company in question. In fact, the company was on the other side of the country in North Carolina, and all of a sudden, they had an IRS problem that they had to clear up. So they hired a lawyer. They wanted to try to fix it. They kept getting more and more letters from the IRS. They had to try to contact authorities, this is in 2003 and 2004, to see if something could put an end to this individual who was impersonating the Californian and

continuing to earn money, but, of course, it was the Californian who was being asked to pay the taxes.

And then the problems continued to multiply because the individual whose identity had been stolen by this illegal migrant started to receive calls from collection agencies for medical, furniture and cell phone charges. The individual's husband recalled that these collection agencies would telephone as many as eight times a day. "My wife would jump up every time the phone rang. In the middle of the night, she would wake up afraid and just sit up in bed."

This is the very real cost of identity theft, even when it turns out to be an identity theft committed to enable an illegal migrant to work in a way that's unauthorized, and by the way, for those who wonder where the impact falls, the statistic in the *Wall Street Journal*, which is somewhat surprising, is that about 53 percent of all Latinos who were victims of identity fraud in 2007 reported that the fraud involved opening an account in another person's name and Latinos are 1.5 times more likely to have an account fraudulently opened in their name than are fraud victims of other ethnicities and that's because of the comparative large number of people with -- from Latin countries who are working illegally in the economy.

So here again, we see that even when a single individual commits an identity fraud and even when it's in the course of an illegal employment rather than a much more sophisticated scheme, people have real consequences to their reputation, to their finances and to their peace of mind.

So how do we deal with this issue of identity management? Well, here in the first decade of the 21st Century, our basic strategy of dealing with protecting our identity hasn't changed very much, frankly, from what it was in the last century. We basically rely on two types of ways of protecting identity, sometimes separately and sometimes we use them together.

One is a card or a document. The passport is generally regarded as the gold standard. We use driver's licenses. Anybody on a college campus, and don't raise your hands if you know about this, probably knows where to get a false ID in order to drink. So that's certainly a much less robust form of protection than a passport and sometimes we allow people to identify themselves using documents that are even unofficial. So that's one method that works imperfectly.

The second method is what I call the secret information method. It's the use of some number or some word or something that's like a password that is meant to authenticate you as the genuine person who is entitled to engage in a transaction or work or access a bank account.

It's because of this secret information type of identity management that we often read in the paper about laptops being stolen and then people worrying about their identities being stolen as well because the laptop has a name and a social security number.

The difficulty with the social security number is not that there's anything intrinsically private about it. It doesn't reveal personal details about your preferences and what you read, but it's that the more we rely upon a number as an identity authenticator, the more dangerous it becomes to lose control of the number and yet if you think about it, using a number or a word as an authenticator carries its own inherent vulnerability because as you give the number to the people who are going to authenticate you, they now have the number and the more people that have that number, the more easily they will lose it.

So you can see both of these methods, a card that is easily forged or counterfeited or a number which can be lost or misused, both of these are imperfect ways to protect identity and, frankly, it's this imperfection that has led to what I think is increasing stories about identity theft and an increasing concern.

Now using 20th Century tools, we are doing some things now to try to strengthen our ability to protect identity using these two methods, but what I'm going to say to you shortly is that I actually believe in the 21st Century, there's a better way to do it and one that's ultimately going to replace what I consider to be a comparatively primitive way of protecting identity.

The first thing we do, using again traditional 20th Century methods, is we try to make it harder to counterfeit a card and this is a pretty good approach if you're going to use a card-based identifying method by itself. We've put chips in passports. We've created pass cards. We've put bar codes in. We've embedded certain kinds of holograms, all of which are designed to make it more difficult for people to fabricate these cards, and we've required higher standards through things like our Western Hemisphere Travel Initiative which governs what people need to show when they cross a land border or our Transportation Worker Identity Card or even the Real ID Initiative to strengthen the security of our driver's licenses.

But while this has done something to deal with the issue of forgery and counterfeiting, it's certainly not a complete solution because time and again, I certainly have seen intelligence that tells me that sophisticated criminals and sophisticated terrorists spend a great deal of time learning to fabricate and forge even these improved cards. The net effect of this may be that it's going to be harder for people on campus here to get a drink when they're under 21, but unfortunately it's not going to be that much harder for the most sophisticated dangerous people to counterfeit an identity card.

With respect to the vulnerability that we experience when we give people our social security number or our PIN number, again here a partial solution that works somewhat well is encryption. If you encrypt, if you safeguard, then you do in fact minimize the possibility that someone is going to steal your number and therefore make off with it.

But I want to remind you, every time you get on a telephone, you give your credit card to somebody in a company as a way of validating your identity, you are trusting that the person on the end of the line is not going to misuse it. That's part of the inherent vulnerability of secret information as a sole identifier.

So I think that we are taking steps now to deal with the issue of these identity vulnerabilities. I think they are partly successful, but I think in the long run, they have inherent vulnerabilities that suggest they may not be a complete solution.

Now some people take a totally different tack. They actually don't want us to do anything at all to improve identity management by either creating different or better cards or collecting more information or doing anything of that sort. They take a general privacy objection to all the efforts that we are undertaking and the efforts I'm going to suggest we should undertake with respect to securing our identities and giving us greater confidence that we can identify people and we can -- people can identify us.

And before I go further, let me tackle these objections straight on. The first objection is, I think, probably the most persuasive from a policy standpoint and that is the argument that you have a right to anonymity, that you shouldn't be required to identify yourself willy-nilly. We can walk down the street without having to justify that to anybody else.

Now, you know, there's a lot of appeal to that in certain settings. I, too, believe, that absent something extraordinary, you shouldn't have to identify yourself walking down the street of Los Angeles and have a document that can verify that you are who you say they are -- who you say you are.

European countries, by the way, differ with this. They require that you carry -- many of them require you carry an ID card, but I think there's a good case to be made that at least in an open street, in an open forum, you should be able to move along without having to identify yourself.

At the same time, I think very few people would argue that you should be able to cross a border without identifying yourself. Most people understand that when someone wants to come into our country, we have a right to know who they are, so we can make a judgment about whether we want to let them in or not and that's true in the same way that we have a right to determine who enters our house and, by the way, that's why when the gas meter reader comes to the door or someone comes to the house in order to perform some kind of a health inspection, you ask for identification because you want to verify the person is who they say they are. So that's the context in which anonymity, I think, doesn't make a lot of sense and isn't very persuasive.

And now, of course, we require identification to get on airlines. Some people may think that that's wrong as well, that we should not require people to identify themselves before they get on an airplane. You understand why we do it, because we know there are people out there who are dangerous, because we would not want to have Mohammad Atta's training camp roommate getting on an airplane where other people are flying and turning it into a weapon or blowing it up, and so therefore from a security standpoint, anonymity has to give way to the right of others on the plane to feel safe.

I've two responses in particular to people who argue with this proposition. One is empirical and one is kind of a philosophical response.

The empirical response is that I think that if you -- if I could run a market experiment, I would set up an airline that is an anonymous airline that allows people to get on without identifying themselves and then I would watch to see how many people decided to fly that airline as opposed to the airlines where people do have to identify themselves, and I think the answer is very few would fly that airline, and I also think you'd have a lot of problem finding pilots who would fly the airline because people understand that that identification is necessary to protect themselves and that gets me to my philosophical argument.

Often the people who argue for anonymity don't recognize that there are two people in any transaction where a person is asked to identify themselves, the identifier and the person who is asking for identity. Both of those people have rights. A person may have a right to control whether they disclose their identity, but the person who's transacting with them has a right to know who they're transacting with.

It's what I call the caller ID model of identification. When caller ID was first distributed widely, there were people who objected on the ground that if you didn't want to identify yourself as the caller, you shouldn't have to have that appear on someone's screen and the solution that was developed, I think, is very clever and very fair and in many ways my model for how we ought to deal with the issue of anonymity across the board.

The model is to give the caller the right to make themselves anonymous, to have on the screen in lieu of a number something that says caller unidentified or refuses to identify. So that protects the caller's right to keep themselves anonymous but the person being called has the right to see that and before they pick up the phone to say, you know, I don't want to deal with a person I don't know and therefore the caller doesn't get to complete the call.

So both sides, the identifier and the person asking for identity, have their rights safeguarded and that's my view really with respect to the issue of anonymity on the airplanes.

The public has a right to know before they get on the plane who's getting on the plane because if they're told that we're going to be letting people on the airplane who don't identify themselves, they're probably going to get off that airplane and that's why I think we are going to continue to see a requirement of identity when you get on airplanes.

The second issue that's raised sometimes is the issue of, well, yeah, we agree that you should be required to identify yourself, but it's wrong to have the government set the standard for what that identity document ought to be.

I have to say this is kind of a silly argument. If you believe that it's fair to ask someone to identify themselves, there's no argument in favor of making it easy for the person to do it with a false identity. Lying and deceiving are not values we generally try to promote in public policy and there's certainly no reason to let any of you -- for any of you in the audience to welcome someone else impersonating you in order to access your bank account or get on an airplane or exercise some other privilege.

The third argument, and the one I'm going to talk about when I discuss -- turn to the last part of my remarks which is what I think we can do in this new century, is the increasing problem that I alluded to earlier of theft of data and forgery.

These objections, I think, are the ones that are the most practical objections we currently face as we deal with how to manage identity and they're actually objections to which I believe we can develop solutions and so to explain what the solution is, how I think we can reconfigure our identity management system to minimize theft of data and further minimize forgery and further safeguard identity, let me stand back and give you a sense of what I see as the universe of tools that we have available for managing identity.

I like to say that the issue of identity authentication, determining that you are in fact the person you claim to be, really rests potentially on what I call the three Ds: description, device, and digit, and what do I mean by that? Well, description means some piece of information or something known to you and not to anybody else that can separate you from the other person who claims to be you.

As I've indicated, standing alone, this has a vulnerability but it doesn't mean that it can't be used in conjunction with other kinds of tools, like device and digit.

The second is device. Now, the device we most commonly use to identify ourselves is the card, the card that can be forged in some cases, in some cases may be harder to forge, but there's no logical reason that only a card can be used as an identification device. A cell phone could be used as an identification device. If you constructed a cell phone and you created a token in a cell phone and the way the token system works, if you operate in the area of intellectual, you know, property and IT, is the token changes every 30 seconds, so that the number that flashes on the token is useless if it's stolen because in 30 seconds, it doesn't grant access anymore.

Now many of you actually use cell phones as identification devices now because you can get on the Internet with your Blackberry and you conduct business using your Blackberry cell phone over the Internet. You're using an identification device. So this is not some startling insight by me. It's a recognition of where we're headed.

The third potential strategic leg, besides description and device, is digit, your finger, your fingerprint, more commonly described sometimes as a biometric. Your digit is unique. Your fingerprint is unique and the ability to use that as an identifier, as we do, for example, throughout the criminal justice system, gives us a third powerful tool that we can use in order to make sure that we can separate real people from impersonators.

Now what I'd like to suggest to you is that the way forward is to work with all of these tools in combination, to take the ability to use some descriptive information, like a PIN, or some private information, a device like a card or perhaps a cell phone or other electronic device, perhaps with a token, and a biometric, like a digit which is easily used and concurrently be captured on a whole host of mobile devices, to combine these together and I can envision a time in the not-too-distant future where, in order to authenticate yourself, whether it's for purposes of getting on an airplane, whether it's for purposes of transacting business at a bank, whether it's for purposes of gaining entry into a student dormitory, that you will have some kind of device, it may be electronic, that will combine two or three of these three Ds, as I call them, to increase the ability to be secure in the knowledge that nobody else can duplicate your ability to identify yourself.

And I think this is the way forward on the theft and forgery issue. Now, some people say, well, of course, it's not perfect. I mean, there will be some people who will be so good that they will be able to somehow -- you know, they'll steal your device, they'll find a way to get your fingerprint and fabricate it and then they'll somehow ferret out the piece of information and having assembled all these things, they'll be able to impersonate you.

But, you know, nothing is perfect. If the test of any movement forward in a system is that the new system has to be perfect, we wouldn't have airbags in automobiles. After all, the airbag is not perfect. If you run headlong into an 18-wheel tractor-trailer, that airbag is not going to help you. But in a lot of accidents, it will help you. So I'm arguing this is a 99 percent solution and in real life that's a very good solution.

I'd also like to suggest that there's some additional things we can use to protect privacy and that involves, first of all, increasingly using the caller ID model where both sides get to make a decision in advance whether someone's going to identify themselves. I think, by the way, that's the model in a sense we use on airplanes these days.

One of the things TSA does is it says, you know, if you want to travel on the airplane, you have to identify yourself and that's because of the interest of everybody else on the plane. Now, you don't have to identify yourself at the airport but then you can be refused entry on to the airplane, and as I say, I mean, I wait for the day that an airline comes forward and proposes that they have an anonymous airline.

A second thing we can do is move to a system in which in fact there's a third party who validates identity so that neither the identifier or the person requesting identity actually has to -- the person requesting identity doesn't actually have to see the identifier's information but they get validated from a third party.

This is sometimes called in the non-technical term the "ping" system, P-I-N-G. It's used -- the Europeans use this a lot when they want to validate identity. They check against the third party database. The third party doesn't know who's checking and who's being checked, but they do know they're getting an inputting request and an inputting authentication and then they validate to both sides. This is a form of distributing the information, and I think a lot of people, I know in the tech world, believe that distributing the information is another way forward to protecting privacy and protecting security without sacrificing the benefits of being able to authenticate.

So this is what I think the way forward is in the 21st century, which I think will deal with what I believe is the last really serious objection that we have to our identification methods which is the remaining concern about theft of data and forgery and here's my challenge.

I think this is not a task that the government alone should do. It is my belief the government should set performance metrics on the capabilities that identification must have. Now sometimes we issue identification, we issue passports, we issue licenses, but certainly for things like getting on airplanes and getting in buildings, I would challenge the private sector to come up with methods and forms and systems of identification that would meet these performance metrics, that would accurately identify a person who's been validated, working from a respected breeder document or some kind of database that truly verifies and validates identity, and that satisfies the security measures because I believe that we should then be in a position in the government to say we'll accept that identification.

If someone comes forward with a really good identification, I-identification, like your iPhone or your iPod, that meets these metrics, we should take it at the airport. We should take it in federal buildings. I think we need to unleash the technical skills and the systems engineering skills of the private sector to tackle a problem that we are still fighting using 20th century means.

So that's my sense of where we are going in the 21st century and what I continue to believe will be very much at the heart not only of homeland security but at the heart of economic security, at the heart of personal security, and dare I say very much at the heart of protecting our reputation and our privacy which are very much the foundation of our liberty.

Thank you very much.

**Secretary Chertoff:** All right. So now I'll take some questions and I'll ask if you'll wait for the microphone.

**Question:** Sir, hasn't the James Bond series showed that digital prevention of fingerprints is obviously superseded by wearing a thin latex glove with somebody else's fingerprint on them and then accessing anything you want?

**Secretary Chertoff:** See, and here's the answer to that, the answer to this which will cleverly be put together by people in the technical world is that, first of all, when you put your finger on a digital reading device in the presence of someone, they're going to look at your finger and they're going to say, what is that funny gummy thing you have on your finger that's being used to replicate a fingerprint? Or, if we're going to use remote fingerprinting, what we're going to do is — and I think

this capability exists — we're going to put into the device that's the fingerprint reader something that measures your body temperature and is going to light up if there's some discrepancy or something that raises an issue.

The one thing I'm confident of is this: any technical threat can be met with a technical solution, but I'll reiterate what I said earlier. There's no 100 percent effective thing and I'm never going to tell you that there will be a 100 percent effective thing. But frankly, if you could reduce identity theft by 99 percent, you'd be way ahead of the game.

**Question:** Mr. Secretary, you mentioned the impact or the effect of illegals working and obtaining false identification. Do you think we'll ever have a guest worker program that works like they have in some of the European countries?

**Secretary Chertoff:** Well, I don't know that it works in the European countries, but the answer to that is I believe we will. We tried very hard last year to get a guest worker program which I continue to believe is not only necessary for the economy but it is actually a way of enabling the enforcement.

I mean, there's obviously a straightforward solution to the problem of illegal work, which is you open the front door and you shut the back door and then the people coming through the front door, you know, you check them first because you have a right to invite people in your own house. You give them an identification card. You know who they are. They're protected because they're not working illegally. The employer pays tax and everybody's happy.

Congress wasn't willing to open the front door. It's opened a little bit, but it's not really wide open.

In the interim, to be honest, we're closing the back door and we're doing it because (a) it's the law and (b) I think it's a necessary condition to satisfy the American people that when the front door is opened, we will really bring people only through the front door, but, you know, I'm ready, willing and able any time in the future to get up and work with anybody who wants to get this thing done.

It's a sad thing that, despite overwhelming support for a balanced program, we weren't able to get it done. Government probably has had to devote, you know, effort to re-establish its credibility which we've done, but it's, you know, a tough process.

**Announcer:** Please stand up and identify yourself. Thank you.

**Secretary Chertoff:** There you go, humor. It's identity humor. It's really --

**Question:** I'm Yvonne Kinman. I have a question regarding a recent article in the L.A. Times.

**Secretary Chertoff:** That's always a dangerous predicate to a question.

**Question:** And this is their wording. "The government is in the habit of losing laptops frequently with personal information."

Now, my question is what is the standard of accountability of this kind of negligence in light of we're spending this much money on computer chips and holograms?

**Secretary Chertoff:** Well, of course, the problem with losing laptops is -- first of all, it's not limited to the government. The private sector does it, too. There was a story where a registered travel company, a laptop disappeared.

It's a hard problem. There should be accountability. People do get disciplined when they misuse a laptop. But actually, you've put your finger on a deeper issue which I'll talk about for a moment.

When you build a security measure, it has to be built in a way that works with the natural habits of people in terms of efficiency. The easiest way to prevent laptops from being lost would be to prohibit them from being removed from the workplace. Why have a laptop then? You just use a PC. The purpose of the laptop is to be able to take your work home with you.

Now, you can tell people, encrypt the data, don't lose the laptop. A vast majority of people honor that, but time and again someone fouls up. There have been stories going back historically of -- I think there's a story over in Europe of some very significant disks being lost because someone left them on a train.

You've got to build the system with human nature in mind. There's not -- it's not going to be perfect. There are going to be mistakes and that's why I come back to my issue of personal information. Putting aside the cost of the laptop which is, you know, I know \$500, \$1,000, the real problem there was it had personal information. Some of these cases involve personal information.

Now, some of it's truly intrinsically personal, like medical records and things like that, but sometimes what's being lost is a

social security number. My position is I'd like to see us in 10 years in a place where you don't use your social security number to identify yourself and therefore if somebody gets it, it's not going to do them any good, just like if someone gets your name, they're not going to be able to walk in and say I'm so and so, you know, I want to withdraw my money from the bank.

At bottom, though, any security system is going to depend on people. It has to be built in a way that takes account of human nature, has to take account of the fact that there will be mistakes, and you're right in reminding us that as we spend a great deal of effort, for example, dealing with hackers and trying to build complicated systems in terms of, you know, what goes into computers to make sure we're not getting bad code, in many cases, the most vulnerable thing is the human being who carelessly leaves the laptop on or lets it get stolen and that's why this is a hard issue and the solution set involves a lot of different pieces, but I think that what your point illustrates is the importance of trying to build a system that is capable of being resilient in spite of what will inevitably be human mistakes.

**Question:** Hi. My name's William. Secretary Chertoff, thanks for coming out.

Considering the amount of people that are on, say, no-fly watch lists mistakenly and unable to correct that status, could you suggest ways to safeguard the government and law enforcement would use the information efficiently and in a trustworthy manner and the people be protected from the government misusing that information?

**Secretary Chertoff:** Yeah. Let me tell you, you raise two separate issues. One is the issue of false-positives on watch lists. Contrary to some of what you read in the paper, the actual watch list in TSA is many orders of magnitude less than the figure of a million which was mistakenly put out.

But the issue of false-positives goes back to the name. We are a name-based identification system and many of us have similar names. You know, John -- there's a lot of John Smiths in the United States. If there is a John Smith who is on a watch list for good reason, the challenge is how do you take the other John Smiths off that? How do you remove them from being mistaken or positively identified as that John Smith?

Now, there's actually a simple solution to this. If you can get from the innocent John Smiths their date of birth or some other additional unique identifying fact, you can put that into the system and then when they present identification, they're immediately taken out of the system. Basically, they're excluded from the set of people on the watch list, and we actually in May changed our system to deal with this issue for people who are in selectee status which means they were automatically being put into secondary and they couldn't get their boarding passes without going to the desk.

We told the airlines that we would allow them, if someone gave a birth date, to exclude that person basically from the list and to let that person get their boarding pass directly at home or in the kiosk like everybody else. Some airlines have done this. Some airlines have chosen not to because they don't want to spend the money and their attitude is, well, TSA gets blamed for it, so, you know, I guess they could do what they're doing now with food and they could charge you for it, but I hesitate to suggest that, I may give them an idea, but the bottom line is there's a solution which involves using an additional identifying fact to take people out of the category of the person who's watch listed.

The end state solution is going to be to do what I said earlier which is to have a third party validator. We are very close to issuing a rule which, frankly, we've been trying to get permission to do for some years called Secure Flight, where TSA would actually become the validator, would match the list.

Right now, the airlines do it. So we could internally correct the false-positives with this data and what would happen is the airline would send the manifest and we would simply see whether the people on the list are the real bad John Smith or not the real bad John Smith and then we'd clear everybody else. We wouldn't be interested in where the cleared people are going and the airline wouldn't have to maintain and deal with the issue of that list.

On the issue of people misusing information, you know, when people steal information or something of that sort, it's actually punishable. I'm actually not aware of many cases where people in the government have deliberately stolen information, personal information. There are regrettably more cases where people have negligently mishandled it or somehow lose it or something of that sort.

Let me go way in the back there. Just so you know because the lights are in my eyes, I can't really see anybody out there. I just kind of look where there's movement.

**Announcer:** Mr. Secretary Chertoff, you have five more minutes. Thank you.

**Question:** Thank you. My name is Scott Gallagher. My question regards while I understand and I appreciate where we're going with this, what do I do currently, especially when companies are hiding behind the Sarbanes-Oxley Act when it comes

to identifying me?

For example, a recent phone call. I call the company and I say I want to talk to you regarding this information I just received from you in the mail and then they begin to vet me to make sure that they're talking to the right person and all the identifying information they're asking me is on the piece of paper that I held in front of me.

Now, if somebody has broken into my PO Box and stolen this, they're getting -- they have all the questions and I will ask them to please find another way to validate me and they say that they can't or they won't.

**Secretary Chertoff:** Well, see, that's -- but that's a great example of this point of using multiple systems. That's the -- you know, they're still stuck on the old secret information system. They're probably a little stupider than most because many companies don't put all the information and they require you to use something like your mother's maiden name or something of that sort.

But again, if we moved away from that system into a system where you could electronically identify yourself or you could use a combination of things, the concern you have would be abated.

I should say, by the way, not every issue requires, you know, the same robustness of identification. Buying a movie ticket doesn't require anything and it may be that some of this stuff you don't care very much about, but on anything really important, with personal, getting access to personal information, there should be multiple forms of authentication to avoid precisely the problem you've identified.

**Question:** Secretary Chertoff, I agree with your comment about we need a validation agency of some type, particularly with regard to electronic communications. I'm also concerned also that it would be solely a governmental activity, but haven't we overlooked a constitutional duty and responsibility to have, let's call it, a national electronic postal service? They would do things like issue electronically watermarked postmarks. We could do -- we could even establish systems on computer-maintained files so that we would have privacy issues secured as well.

Do you look at this as we've overlooked a vital organ, if you like, in our attempt to have security in telecommunications by not having a national electronic postal service?

**Secretary Chertoff:** Well, I'm happy to say one of the very few things that's not in my department is the Postal Service.

**Secretary Chertoff:** But I don't know about a national electronic postal service. I will say, and I think after this I have to depart, you're right that the Postal Service is underutilized in this respect. I think people are moving more to electronic mail and private services, but the Post Office is now increasingly a place where you get a passport.

The process of getting a passport, you know, that is still regarded as the premier validation document. It's a document which, if you present, should allow you to get other documents that are more convenient and one of the things I hope to see is, as the Post Office re-engineers itself over the next, you know, few years, that they increasingly look at whether they can be in the business of servicing identity management. They can -- because every town has a post office.

You know, I've learned a lot about systems engineering. The biggest problem is getting physical things distributed widely and the Post Office is the government's leading physical -- other than schools maybe, the only institution that exists literally in every town. We've built it. We've got people working there. So I think in the long run as we're getting into this 21st century model of identity authentication, I think that's definitely a resource that ought to be used.

Thank you very much.

**Dr. Nikias:** Thank you. Let's give him a round of applause. Thank you. Thanks for joining us, Secretary. Thank you.

This page was last reviewed/modified on August 13, 2008.