Remarks by Homeland Security Secretary Michael Chertoff to the 2008 RSA Conference

Release Date: April 8, 2008

San Francisco, Calif.
Moscone Center
RSA Conference

Secretary Chertoff: Thank you for the very warm welcome. Thank you for the music. I think it's the first time I've made an appearance at a speech where I was preceded by rock and roll so I may adapt this now and use it in the future. I'm delighted to be here and to have an opportunity to address you as well as to have the opportunity to meet with a number of senior executives in the industry shortly before I came out -- and that's because one of the critical concerns we have to address in this country is enhancing our cyber security. That's a major area of focus and attention for us this year, and I want to have the opportunity to talk to you a little bit about what we plan to do.

Last month our department celebrated its 5th anniversary. As you'll recall, we were created five years ago to mobilize the nation to prevent, protect against, and, if necessary, respond to terrorist attacks as well as natural disasters. Of course, the immediate incident which spurred the formation of this department was the terrorist attacks of September 11th. But we quickly came to realize that we have to look not only at those threats that have materialized in the past; we need to consider those threats that could materialize in the future. And there's no question that one of the threats which continues to materialize again and again in the private sector and in the government is the threat to our virtual world of cyberspace. It's a world in which we're not likely to see airplanes crashing into buildings, but we could see human and economic consequences that are very much on a par with what this country tragically experienced on September 11th, 2001.

We take these threats to the cyber world as seriously as we take threats to our conventional, real, physical world. We know that a successful large-scale cyber attack against our country would have very far-reaching consequences, precisely because we all depend upon the Internet and other computer networks and systems to conduct virtually all of our activities, public and private. Because of the interdependence of our society and our economy, a cyber attack would have cascading effects across the country and across the world.

But while the potential consequences of a cyber attack are very real and every bit as concerning as the potential of a physical attack on the order of what we saw on September 11th, managing the risk of a cyber attack is not quite the same as managing the risk to our airline system or our transit systems or our borders. For starters, cyber security is not solely a federal responsibility. The federal government does not own the Internet, thank God, and it doesn't own the nation's cyber networks. You own the Internet and the nation's cyber networks. The federal government cannot be everywhere at once over the Internet or in cyberspace. There is a network that operates within that domain. And as a consequence, the federal government cannot promise to protect every system, let alone every home computer from an attack.

Moreover, as you know, cyber threats don't come in simply one variety. They include a very broad range of nefarious activity -- from a single individual acting as a hacker to an organized criminal group trying to steal personal or financial information to exploit for ill-gotten gain, to a hacker trying to breach a system simply in order to show that he or she can do it, to nation states engaged in cyber espionage against governments and businesses. And, finally, there is certainly the prospect of a terrorist group seeking to highjack and exploit the Internet to cause very real world damage to our systems and to our country.

So I'd like to take a little bit of time today talking about the nature of the cyber threat we currently face; how we are currently managing it from a federal perspective and in partnership with the private sector. But I'd also like to talk about a vision for where, I think, we need to go if we are going to truly live up to our responsibility to protect this network which is very much the foundation of modern economic and personal activity.

Let me caution you, of course, that a lot of the work that we do is classified, so I'm not going to be able to discuss in detail everything that we are doing or that we plan to do. But I do hope to leave you today with a reasonably clear picture of what we can and must do to protect our country against growing threats in the cyber world, the steps that we're currently taking and, perhaps most important, the steps I think we need to take in the future.

Let me begin by being a little bit more specific about the kinds of cyber threats we're worried about. Obviously, these threats don't necessarily occur in a way that's visible to the naked eye, although the threat -- the result of these threats, the consequences of successful attacks can be very serious in the real world.

Cyber threats are also decentralized. The leverage that even a single, skilled individual has to cause mass havoc is enormous. In that sense, cyber threats have enabled terrorists and criminals to do a kind of damage that they would never really be able to contemplate doing in the real world. Let me give you an example. Last May a botnet attack in Estonia essentially shut down the Estonian government for a period of time. It affected their financial system, it affected media websites, and this occurred over the course of two weeks.

According to the Estonian government, more than a million computers were involved in the attack. Our own government websites that usually receive a thousand visits a day -- I'm sorry, Estonian government websites that usually received a thousand visits a day were inundated with 2000 visits a second. This attack went beyond simple mischief. It represented an actual threat to the national security and the ability of the Estonian government to govern its country.

Now, we worked with the government to help them respond and avert further threats. But the attacks on Estonia are simply one example of what any government of any country could face if determined terrorists or other mischief makers decided they wanted to carry out cyber attacks against our institutions. And so we face in the 21st century a very difficult problem: a single individual, a small group of people and certainly a nation state can potentially exact the kind of damage or disruption that in years past only came when you dropped bombs or set off explosives.

Moreover, we may not know immediately or for some time who caused the attack, which makes the traditional model of deterrence one that works only imperfectly in preventing people from carrying out this devastating warfare against our computer systems.

Let me say that we break down the kinds of challenges we face in the cyber world into three broad categories. First, there is the traditional effort of criminal groups to find where the money is and try to exploit what they can in order to get that money for themselves. And so we have criminal groups that attempt to highjack the Internet or penetrate networks or systems either to extort money as tribute, or in order to collect valuable financial information they can use later in order to pillage people's bank accounts or financial assets. And this is merely a 21st century version of a kind of threat we've traditionally dealt with.

A second order of threat is the theft of information: espionage. Again, this can be done both from a governmental standpoint -- those who want to see what our secrets are -- or it can be done from an industrial standpoint; those who want to steal the crown jewels of our asset base, our intellectual property.

And finally, and perhaps most troublingly, there is the threat of somebody penetrating our systems not merely to obtain criminal gains or to steal our information, but literally to shut the systems down. Imagine, if you will, what would happen if a sophisticated attack on our financial systems caused them to become paralyzed. There would not only be the short-term consequences to the systems themselves, but there would be a shaking of the foundation of trust on which our commercial and financial intercourse depends. Imagine what happened if it were possible for hackers to enter an air-traffic system and play with the system so that it was no longer reliable, so that we were forced to ground aircraft, so that it caused a crisis of confidence in our air travel system. It's easy to see that from the standpoint of a terrorist, this kind of attack might yield the sort of real world consequences that we've previously seen only when we imagine physical destruction of the worst kind.

So we face a very serious challenge and one which, I have to say, is only likely to grow more serious as time passes. And as we tackle this challenge, we have to recognize that we're operating in a domain in which traditional military power, or the power of government, is insufficient to address the full nature of the threat. Because we are dealing with network systems, a command and control response will simply not be adequate. We need to have a network response to deal with a networked attack. Put another way, it takes a network to beat a network.

Now, with that picture of the threat in mind, let me tell you what we're doing. But let me also be candid about where I think we have fallen short and where we need to go in order to enhance our level of protection.

Several years ago when the department was created we established a National Cyber Security Division to manage cyber threats, and as part of that we created US-CERT, our Computer Emergency Readiness Team. US-CERT provides 24-hour, early-watch warning and detection for the federal government's Internet infrastructure. And we have also worked directly with industry to analyze and respond to cyber threats and vulnerabilities. US-CERT, for example, was involved in helping the Estonians combat the attack that they suffered some months ago.

Certainly, US-CERT has added value to the protection of federal domains and, in partnership with the private industry and the private sector, to help strengthen our defense of private domains. But I cannot tell you that it has been sufficient, particularly in an evolving era where those who would cause us harm are continually adapting and refining their techniques so that they can be more skillful at the kinds of damage that they want to carry out.

Therefore, the time has come to take a quantum leap forward; to really engage in what I would call a game changer in how we deal with the issue of attacks, first and foremost on the federal government, and then secondarily working with the private sector to protect all of what we depend upon in our modern world.

In January of this year the President signed a joint national and homeland security directive building on efforts to date and directing that we formalize and implement a national cyber security initiate. This is -- I don't want to overdo the analogy, but it would almost be like a Manhattan project to defend our cyber networks in the same way that we've undertaken previous efforts in the past to deal with emerging threats. Under this strategy, this department and others lead the government's efforts to protect the federal domain and ensure the security, resiliency and reliability of the nation's information, technology and communications infrastructure.

So how do we find ourselves in the federal domain as it relates to security against these kinds of attacks? Well, as I've said, we currently have US-CERT, which works with federal agencies across the civilian elements of government, to help analyze attacks and respond as quickly as possible. But US-CERT and the particular intrusion detection tool that they rely upon called EINSTEIN is limited in its efficacy by three constraints.

First, we currently have literally thousands of entry points into federal civilian domains from the Internet. That means it is not possible for us to monitor everything that is entering the federal domains in real time and effectively because there are so many access points through which the world at large and the Internet at large can enter our federal networks. That has limited the ability -- our ability to be completely effective.

Second, federal agencies themselves are uneven in the way they protect their own assets. Some do have 24/7 watch and warning situations, op centers, that allow them to respond effectively when we notice an anomaly, for example, and we want to notify them that they may be attacked and we need to respond. But some agencies do not have 24/7 watch and warning. And it should be perfectly clear to everybody in this room that while it may be three o'clock in the morning in Washington, it's not three o'clock in the morning on the other side of the world when an attack is being launched. So this is an additional constraint.

And finally, the architecture of EINSTEIN is fundamentally a backward-looking architecture. We identify anomalies by looking at traffic that has penetrated or entered certain federal domains. We analyze that to see whether we believe there is something nefarious going on. We contact the agents and we ask them to look at their own networks. And then when they come back to us, if we determine there's an attack, we try to take steps to identify the signature and characteristics of the attack so we can identify it if it comes in the future. This doesn't happen instantly, and the time delay in all the steps of the process I've told you is time we cannot afford to lose in a world in which attacks come literally in microseconds and from all points of the globe. So these constraints have limited the effectiveness of our ability to deal with an increasing tempo of attacks on our federal civilian domains.

So what is our strategy to dealing with this? I think we need to deal with all of these constraints, and we intend to do so in partnership with other federal agencies as the first step of the President's national cyber security strategy.

First, we need to reduce the number of access points to our federal domains. We have to consolidate our external connections to federal government systems. This concept, which some describe as a trusted Internet connections initiative, allows us to identify a finite number of entry ways into the federal systems so that we can effectively monitor the traffic over those entryways. That gives us better visibility into what is coming into the system and a better ability to see whether something dangerous is trying to penetrate. Our goal is to reduce access points from a current number that ranges in the thousands to a target of about 50.

The second element is we need to use our accreditation and certification authorities, which we exercise in conjunction with OMB, the Office of Management and Budget, to assure that all federal agencies bring their capabilities to detect and respond up to a minimum baseline level that assures that there is a 24/7 watch and response capability. As you know, once you enter what some describe as the cloud of a network, the network is only as strong as its weakest link. We are interdependent in the federal system. An agency that allows itself to be vulnerable because it's not swift and certain in its response is an agency that has created a portal to subverting the security of the entire system.

Third, as we build these capabilities in the agencies and as we reduce the number of access points, we need to drive our technology and our operations to a faster cycle time awareness of attacks when they occur. We need to be able to detect and analyze anomalies not in hours but in minutes, and to take an effective response in a very short period of time thereafter; a response that includes not only mitigation through resiliency, but warning others who might be subject to attack, and other counter-measures that can be used to prevent an attack from spreading.

Finally, I don't believe we have fully engaged the capabilities of EINSTEIN, which is only limited in the way we use it now to detect signatures and other characteristics that suggest a malicious attack is underway. Ideally, I think what our vision is is to work with our partners and other agencies, including the intelligence community, not only to enhance the capability of EINSTEIN to look more deeply at what might be coming through the Internet, but also to have an advanced warning; an early warning system of what might be launched even before it's come.

We all know the best way to deal with an attack on a system is to prevent it before it happens rather than to respond to it after it's occurred. And even giving an adversary one bite at the apple before we discover what the signature is in the metadata or in the payload is one bite of the apple too much. I do believe we have the capability now to detect what might be the signature of an attack before it's launched. And integrating that capability with our defensive systems is a critical element of where we have to head in protecting the federal domain.

This is of course why we have created a National Cyber Security Center. This center, which is now being lead by a successful, proven silicon valley CEO who many of you may know, Rod Beckstrom, is designed to be a form in which we can bring together all of the federal government capabilities in a networked partnership, recognizing that we have distinct and separate legal authorities but that we also bring unique capabilities to the table that we ought to be able to share in a way that preserves important legal protections, but allows us to get the benefit of all of the technology and all of the skills that we can find in the federal government.

DHS has a responsibility to deal with national cyber security for the federal government, and to coordinate that across the federal domain as well as in partnership with state and private sector networks. Through the Cyber Security Center, we hope to be able to bring the skills of the entire federal government to bear as we engage in this process of coordination, not only in the federal domain, but working in partnership with states and locals as well.

Supporting all of the work I've outlined, the administration has put $115 million -- "one- one-five" million dollars into cyber security efforts at DHS this year, and we've requested another $192 million dollars in the President's fiscal year 2009 budget. This will enable us to dramatically increase our staffing, our technical capabilities and our equipment so we can better lay out the job that I've depicted for you.

Now, much of what I've talked about has to do with our responsibilities in the federal sector, where of course job one is to protect the security of federal systems. But because, as I said earlier, cyber responsibilities are distributed across the entire globe and most of them are located in the private sector, and because so many of our national assets are in the hands of private business or private people, we can't be serious about national security or national cyber security without engaging with the private sector. And by that I mean not just those in information technology, but even the kind of traditional power plants and power structures, financial systems, and transportation systems, all of which, while they operate with real-world assets, depend for that operation on the cyber systems which connect them all together.

Because we have such a widely distributed set of cyber capabilities, and therefore such a widely distributed set of potential cyber vulnerabilities, the protection of these systems is not exclusively or even primarily a government function. It has got to be a shared function. It is a function which those in the private sector have a responsibility to engage in partnership with us, because the failure of any single system has repercussions and cascading effects across the entirety of our nation and our economy.

A lot of important work has been done and I want to commend all the companies and businesses that have taken action to protect their systems and networks. Of course, this not only protects the country but it protects the shareholders, the stakeholders, and the employees of the individual businesses themselves. Many of these private sector entities have worked directly with our department on a number of critical planning efforts. Last May we published 17 critical infrastructure specific plans as part of a national infrastructure protection plan. This overarching plan is designed to provide a framework within which the government and the private sector can work together to manage the risk to critical infrastructure such as dams, bridges, power plants, water treatment systems, air traffic systems, and of course information technology.

In each critical economic sector, the plans we have developed with the private sector outline our common priorities, enhance the sharing of information among the businesses and with the government, identify research and development priorities and set goals and implementation benchmarks. In particular, we've partnered with a lot of you here as part of our IT sector specific plan process to help identify critical IT sector functions and establish a framework for assessing our risk, developing programs to protect and mitigate against that risk, and to drive further research and development.

This is all good. But the question you're going to ask yourself is, how do you all fit now into what we are doing for the national cyber strategy? Well, as I've indicated to you, the first phase of the national cyber strategy has to do with the federal government getting its own house in order, and in particular with the federal civilian domains, dramatically increasing our ability to secure the cyber networks on which we rely. But I believe, in the process of doing this, and in the process of working in our National Cyber Security Center with other agencies of the government, we will develop not only useful technology, but useful information and early warning intelligence that we will be able to share with the private sector to enable the private sector to enhance its own networks and its own capabilities from a defensive and security standpoint.

I want to be very clear about this: this is not the federal government coming in to tell you, you must do something. The vision here is the federal government offering you the opportunity, if you wish, to partner with us to get some of the benefit of what we are doing and learning to help you do the jobs that are so important to you. We have no interest or intention of duplicating a system here, like you see in some other countries that I won't name, where the government tries to sit over the Internet and prevent things from coming in that they don't like. That is not what we want to do and that is not what we will do. What we do want to do is enable those who are interested in working with us to be able to get some of the benefit of what we're able to discover and learn so that you can protect your own assets. And I daresay, as responsible corporate citizens and stewards of your own businesses, you'll want to carefully consider that invitation when the time is right, and evaluate whether you think we can bring value added above and beyond what we've already brought.

Let me raise three other issues very briefly because I think this is also part of the cyber strategy. First, the issue of supply chain. In addition to making sure that we're protecting our networks and our cyber assets against the possibility of an intrusion over the Internet, we need to make sure we're not bringing into the systems themselves the very Trojan horses that could be exploited by somebody coming over a network. That means we need to ask ourselves how we can continue to maintain a global system where components are manufactured and programming occurs all over the world while assuring ourselves that people with ill will, or perhaps the desire to steal our intellectual property, are not embedding in those components' trap doors or other devices that can later be exploited for nefarious purposes.

Second, we need to get much more serious about internal security. You can have the best systems in the world for protecting against an external threat, but if you have someone working in your most sensitive computer systems with access to the entirety of the network from the inside, and they write their password down and leave it at a bar one night because they went out for a drink and they forgot it, you don't have much of a security system. And building a culture of security-mindedness and care is an important element of what we do if we're going to deal with this problem in all of its dimensions.

Finally, I want to deal with the issue of privacy. In my view, when we talk about cyber security, we are also talking about cyber privacy. These are one in the same thing. The essence of what we are trying to protect for the ordinary citizen is the ability to engage in transactions over the Internet with the confidence that their personal data cannot be stolen so that they can be impersonated by another person and have their assets or their reputation ravaged.

I don't know that we've always done a good job about explaining that this is an area where security and privacy are not at odds, but they are actually complementary. And part of what you need to engage your creativity in is thinking outside the box about systems that we can put into place so that we don't have to worry that once some piece of information is stolen, now it's an open door for somebody to pillage my personal accounts or get into my personal data. We need to think about ways to use modern technology, including biometrics, to build a series of systems that doesn't impact on the fluidity with which we transact business, but gives us the confidence and the trust to know that we will not be victimized by those who would highjack our personal data.

It's an ambitious menu. Some would say that maybe it's too ambitious; maybe the problem is too hard. The difficulty is the problem of cyber attacks and threats to our cyber infrastructure will not go away. It may be easier to turn to other problems that seem simpler to solve, but I don't believe it's responsible in the government or in the private sector to avert our eyes from a threat simply because it's a challenging threat to overcome.

And that's why I'd like to make a final plea. In addition to all the work that you do recruiting people to do the cutting edge research and systems development in your businesses, I'd like you to try to sell some of your best and brightest to come and do some service in the government. I think Rod Beckstrom is a great example. Getting the kind of talent and creativity and perspective that people who have lived and worked in this arena -- getting that into the government so we can cross pollinate with what we're doing at a national policy making level is the best thing you can do for your businesses, but more important it's the best thing you can do for your country.

I know some will say, well, you know, the government is kind of clunky, it's not particularly cutting edge. I think if you actually look, there's a lot of exciting stuff being done, many -- and much of it not public. And the one thing the government offers you is a lot of responsibility, often at a time that you sometimes wonder whether you're prepared for it.

I can tell you from my own experience as a lawyer. When I left law school I had the opportunity to be an Assistant U.S. Attorney in the southern district of New York; that was a young prosecutor. I got paid a lot less money than I was making at the law firm I left, but I got the opportunity to get into the arena with the best lawyers in the country and hone my skills and make a contribution in cutting edge legal cases. And I daresay you have people in your companies that would relish the opportunity to do the same thing.

So in the days and weeks ahead we're going to continue to look to tap into the private sector for ideas, for insights, and dare I say, for employees as we increase the staffing at all of our cyber security components as we move forth to implement this strategy and as we work with you in the private sector to build a set of security measures for our cyber assets that don't degrade the flexibility and the entrepreneurial-ship and the creativity of the cyber sector, but that assure that the public will trust that sector with the very precious assets and very precious information that has to be part of those networks if they're truly to work.

I appreciate the opportunity to speak with you today. We value your continued partnership, and I look forward to working with you as we keep our communities and our families safe. Thank you very much.

###

This page was last reviewed/modified on April 8, 2008.