Secretary Chertoff Hosts Blogger Roundtable on Cybersecurity

SHARE

Release Date: October 8, 2008

For Immediate Release
Office of the Press Secretary
Contact 202-282-8010
Washington, D.C.

Secretary Chertoff: I'll keep my initial comments brief. As you know, earlier this year the President approved the cyber strategy, which I think is a recognition of the fact that this is perhaps an area of vulnerability we have that remains the greatest challenge for us in terms of addressing.

I think we've done a lot with respect to physical infrastructure. We've done a lot with respect to borders and things of that sort, but the cyber area has been a tough area. And the reason we've been able to tackle it is because we've been able, for the first time, to bring all of the elements of the federal government together in a joint effort so that we can leverage some of the exceptional tools that the Defense Department has along with our ability to interact with the private sector in a way that will not only enable us to secure our government domains, which are the first priority in the near term, but to be able to offer the private sector some assistance and to enable them to secure their domains.

It's not a secret that, you know, if you look at what happened in Estonia, looked at what happened in Georgia, if you look at that massive identity theft that occurred in California that I announced we had made some arrests this past August, we're becoming more and more acutely aware of the vulnerability we have at all levels: denial of service, corruption of information, theft of identity, exfiltration of confidential information. All of these are critical issues.

Let me end by saying that there's a tendency to view the issue of cyber security as being only at the high tech end of the spectrum that this is about preventing people from hacking in over the Internet. And that's clearly part of the strategy. But, you know, there are other parts of the strategy, too. For example, protecting the supply chain.

When we buy software and hardware, particular software and hardware that comes from other parts of the world, are we confident that that is what it's represented to be, that it's not counterfeit, that it doesn't have embedded within it something that is potentially dangerous to the system or that could be used to extract information from the system? So we've got to look at that issue, too.

The issue of insider misbehavior, people stealing passwords or thumb drives or things of that sort from within an organization. That's the kind of old-fashioned type of espionage, you know, human-enabled espionage, but that's also a threat. Protecting the physical infrastructure that enables the Internet, the stations where the routers are located, the various kinds of network, physical elements of the network. That has to be protected, too.

So our approach is to look at this holistically. Our model is, particularly with the private sector, to work with them in partnership to see how we can help them. And I want to emphasize as far as the private sector is concerned, this is a voluntary issue. This is not the government mandating the private sector to do things. It is the government working with the private sector to enable them to protect these very, very important assets.

So with that, I will be happy to throw it over.

Moderator: If I could just ask you to maybe identify yourself before your first question.

Question: Okay. My name is Jonah Czerwinski. Great to see you again, Mr. Secretary. I'm from HLSWatch.com and delighted to be here. You had recently gotten the budget passed, and about $350 million in there for DHS cyber.

Secretary Chertoff: Right.

Question: Could you tell us a little bit about what that is going to go toward? Is it enough for this initial phase of it, and if it isn't, what's been put aside? What do you think we should look for down the road?

Secretary Chertoff: Obviously there’s a big piece that’s classified that’s not in our Department which I can’t talk about. From our standpoint in the next year, it is actually slightly more than we requested. And what we’re doing is we’re building the basic infrastructure. We are taking our Einstein 1.0, which is our current detection tool, we are now upgrading it to Einstein 2.0 and testing it out, and we’re going to be also -- we’re also in the process of looking at turning it from a passive detection to an active detection device, active meaning that we would have the ability to actually stop an attack as opposed to merely warn about an attack..

So the money gets spent on things like equipment, personnel. We’re recruiting -- I think we’ve got over 100 people in the pipeline that we’re trying to bring on, that’s programmers and people who can actually operate Einstein. Some of this will be necessary, for example, for additional space, you know, all the kind of prosaic things you need in order to expand capability -- leasing, you know, various utilities and things of that sort.

It will also enable us to kick in our share to support the Cyber Security Center, which we’re in the process of standing up. So I think that’s where the money is going to go. And what we’re looking to do in the first instance is get our control over the dot.gov domain. We are currently every --someone said to me every 45 days we are reducing by half and consolidating the number of Internet connections. So that is part of the process of getting control of the dot.gov once we’ve consolidated those Internet connections down from what started at as a thousand and we hope will be in the neighborhood of a hundred or two. It will be easy for us to then use Einstein 2.0 as a way of getting real time detection warning, which of course will be a big step forward from the current general model, which is after the fact, we find there’s an attack and then we tell people, you know, how to respond to it.

Question: So a quick follow-up on that if I could. There’s a mention you made of Einstein 3.0 even down the road, which would be shifting us even further down the spectrum from defense to offense.

Secretary Chertoff: No, it’s still defense. It’s like -- it’s just a blocking capability. In other words, right now -- what 2.0 does is if I know malicious code is coming in, it enables me to give a real time warning. Someone described it the other day to me; it’s like a traffic cop sitting on the highway seeing people speed and he can immediately call in and say someone with license plate XYZ is speeding, and give warning down there.

3.0 would allow the traffic cop to make the arrest right on the spot.

Question: Gotcha. Okay. So it would still be prompted by [inaudible]

Secretary Chertoff: Right.

Question: [inaudible] an act by somebody else?

Secretary Chertoff: Right. It would be based on -- it would be when you detected the attack, you would stop it cold.

Question: Thank you, Mr. Secretary.

Question: I'm Jeff Fox from ConsumerReports.org. Thank you for inviting me. We've been tracking for several years the impact of cyber insecurity on consumers, for about four or five years. We estimate that in the past couple of years American consumers have lost at least $8.5 billion to cyber crime. We've also found that there are significant government leaks of ID theft. I don't know if you've seen the September issue. I'll give you a copy afterwards.

Recently, I think about a year ago, the TSA lost about 100,000 records, personnel records. So I'm wondering what DHS is doing, you know, specifically to protect consumers both in terms of --

Secretary Chertoff: Yeah. Let me -- there are two elements to this. One is -- of course, you're always reading about people having information on laptops and their laptops are stolen. And, you know, that's a challenge for every business because you could say, for example, in a business, you can't put information on a laptop. That's a tradeoff between the ability to work with the information in a way that's helpful and securing the information. You can encrypt the information.

But I would actually make the case -- and this is not with the Cyber Security Initiative, but it's another initiative we've talked about -- that part of what we need to do is we need to change from a model in which your assets are controlled by your, for example, your Social Security number, which is a very weak way to control your assets, to a way in which your assets are controlled by some combination of a biometric, a token, and maybe some secret knowledge that isn't kept in a database.

If you -- bear with me for a second. If you had a system where in order to access my bank account you had to use my biometric and a token as well as a number, it wouldn’t matter if you stole the number, because the number wouldn’t do anything for you. It would be like having my name. It doesn’t do anything for you. So I actually think we need to step out -- I mean, in the short run, you want to protect the information by encrypting it and securing it.

But in the long run, I think you want to move away from a model which I consider inherently vulnerable, where the very information that you’re trying to protect is the information you have to disseminate in order to validate yourself. So as you -- the more effective use you make of the information, the more vulnerable you become. I'm suggesting we paradigm shift.

On the issue of theft of data over the Internet, whether it’s wireless interceptions like we had out in California, there again, a lot of the key is encryption. It is a different architecture for how we validate and verify people so that we don’t have -- so that getting a single piece of information about you doesn’t really do any good, because it’s not enough to get you into an ability to corrupt somebody. And of course, part of it is just doing what we can to secure the networks against hacking or intrusions.

But, mind you, you know, it’s not just about hacking. It can be about interception of wireless transmissions. It can be about theft of data by insiders. You know, someone told me that people stick a lot of data on a thumb drive. You’d be amazed how many thumb drives are found on the floor of airplanes, commercial airplanes, because people drop them out.

Question: A lot of the losses that we track are due to malware infections. You can -- you know, they can -- Zombie, you know, a home computer.

Secretary Chertoff: Right. You have Botnets.

Question: Botnets.

Secretary Chertoff: Yeah. What I’m saying is, there’s a whole spectrum of threats. And what I want to encourage is not just to think about the obvious thing or the thing that gets written about, but to look at what I call game changers, ways to actually organize protection of our identity so that we are not so vulnerable to the theft of a single piece of information or a Social Security number, because that is insufficient to allow someone to actually seal someone’s assets.

And I think this is a huge issue. You can tell I’m interested in it because I’m talking about it a lot. And the cyber security strategy certainly is a big piece of that, but there’s some other things as well.

Question: Sorry. Ben Bain with Federal Computer Week. A couple of weeks ago in releasing the preliminary findings of the CSIS Cyber Commission kind of on cyber security for the 44th President, there was some suggestion that the coordination of the government’s cyber security needed to be raised up to the level of the White House, because we’re dealing with something that’s a homeland security threat, a defensive issue, offensive issue, all the way on down the line. Is DHS the place where coordination should happen? And does the Department have the authority necessary to --

Secretary Chertoff: There’s no -- you know, we don’t -- I think the report kind of looks at things as they maybe were a year or so again. So let me tell you where we are this year. First of all, we do coordinate on an interagency basis, and it does involve high-level engagement by the White House, including by the President himself. So at the policy level, this is a matter that’s coordinated by the White House because it’s interagency.

At an operational level, most of the coordination occurs between three actors: the Department of Homeland Security, Department of Defense, and the DNI. And the reason for that is there are three sets of legal authorities that come into play in dealing with this world. There are our authorities for homeland security. They’re the intelligence community’s Title 50 authorities, and there’s Department of Defense Title 10 authorities.

The Department of Defense, as you would imagine, has a lot to do with things going on if we do something offensive. Intelligence community if we’re collecting information overseas, and of course we are protecting the homeland. So I think operationally we now have the three locations where operational activities are going to take place, closely coordinated together, and in general, the policymaking does take place under White House supervision. So that’s really the model we are using.

What I would hesitate to do is create new officials and new layers of bureaucracy. But I think we’ve got to refine that to a very small team that not only coordinates the policy but is able to coordinate the operational activity.

The Cyber Security Center, when it's fully operational, will be the operational forum or meeting ground where the various people operating their authorities will come together. And I think that's going to be efficient. It doesn't respect, though, the fact that legally, you know, the Defense Department is generally supposed to operate overseas. For example, if they start to do domestic law enforcement, that's illegal. Likewise, I'm not sure people would be wild about the intelligence community sitting over the Internet here. So we're trying to respect legal boundaries, but I think we've got a mechanism now that actually does work well to coordinate.

Question: Just a follow-up question then. In terms of the actual authorities, the legal framework that exists, another suggestion was that new laws, new authorities are necessary. Do you think that the current legal framework, current policies are sufficient for doing this?

Secretary Chertoff: You know, you can't exclude as we go along that we may decide there need to be some new authorities and new laws. But I think this is an area where we ought to proceed in a measured way for the following reason. In the area of protecting military assets and government, I think the authorities are quite clear. We have plenty of authority to do what we have to do.

People have raised the question in the commercial domain whether the government should have more authority. I just want to tell you, the architecture of the Internet and the culture of the Internet is one where I'd be very careful before I suggested the government ought to get into -- intrude in a bigger way.

And, you know, we have a history in this country of everybody says let's do a lot, pass a lot of laws and really, you know, do a lot of active stuff, and then everybody repents at leisure. The Internet, maybe more than any other place, has a distinctive culture that you don't want to break in order to protect. So, my suggestion has been we proceed in a voluntary way and we proceed in a 21st century kind of collaborative way.

You know, Rod Beckström, who we brought in to run the Cyber Security Center, is -- I mean, his expertise is in collaboration, and that's why we did that. We wanted someone who was attuned to a different culture of operating with the private sector than the command-and-control culture of the 20th century.

So I wouldn't close the door on new laws and new authorities, but I would be careful. I would be cautious as we deal with the private sector to make sure we're invited in rather than pushing our way in.

Question: Thanks.

Question: Mr. Secretary, John Solomon from In Case of Emergency Blog. Thank you again for having us. I wanted to go back to what Jeff was talking about, the public and the consumer piece of this. I'm clearly a lay person in this, so it may be a dumb question. But I was trying to understand the public's role here and how they should understand the role. In the cyber month, we're talking about both commercial and terrorism as well.

And as the public kind of looks at this and does some of the things that you recommend, is their exposure basically a commercial exposure and worrying about losing money, or are they part and parcel of the country's exposure to terrorism? And how should they look at, and what should they be doing based on?

Secretary Chertoff: I think, you know, I think that's a great question. Of course there's public in your own personal life and there's the business community. The business community obviously, to the extent they operate critical infrastructure, they have a role to be responsible not only to themselves and their own businesses, but to the wider community that depend upon them.

Because we are interdependent. If the power grid goes down because somebody hasn't adequately protected their systems from an IT denial of service attack, that's going to have implications for everybody who relies on that power.

So there's an awful lot the private sector has to do. It reminds me of the Y2K period when the private sector was required to step up and make sure it was protecting its assets.

So part of what we've been in the process of doing is we've set up a committee with the private sector built upon the model that we've been using successfully over the past several years to create a National Infrastructure Protection Plan.

And the idea is to have a -- it's a critical infrastructure coordinating committee that looks in particular at computers and spans all of the sectors, recognizing that each sector is going to have unique challenges and is going to want to look at different kinds of issues.

From a homeowner standpoint or personal standpoint, you know, obviously you don't want your computer turned into a -- you know, taken over by bots and then converted into an attack vector. But on a more prosaic level, you don't want your personal stuff, your financial records exfiltrated. You don't want to have your computer become sluggish and unable to operate.

And, you know, this is really an area -- it is like the disaster area where personal responsibility is important. If you don't change your password periodically, if you don't update your firewalls and your anti-virus, you're just -- you know what it's like? It's like taking your wallet and throwing out on the street. And no one would suggest doing that. No one suggests just leaving your door wide open without a lock.

For many people, that's how they view the computer, and, you know, whether it's -- to make a larger point, whether it's preparing yourself for physical disaster with water and food as we've talked about, John, or whether it's taking reasonable security over your computer, people have got to do this. Because otherwise, they're going to get victimized and then they're going turn and say, well, who's going to help me? And the answer is, it's going to be a lot harder to help them after the fact than if they take reasonable precautions.

Question: Just to follow up and taking up on the preparedness, one of the challenges is to figure out what in fact is the message. You don't want to give too much, but you want to give substantive. And looking at some of the recommendations, for example, creating a strong password, but frequently changing your password. I know as I was doing my Amtrak reservation last night, it's lucky I remembered. I've got a hundred passwords.

Is that realistic? But or is it something that really is front and center should be something that Americans, as a pain in the neck as it is, and maybe there's an opportunity for technology helping us to deal with that, but is really in your mind a very important thing even if it is a pain?

Secretary Chertoff: You know, I think that actually -- this is really again a great question, because there is a balance. I mean, I've seen circumstances where the requirements for getting into the system are so cumbersome that people stop using the system, and that's not a good answer.

I think it's risk management. In a business where there's a huge consequence to having data stolen. Like in our world. In our world we're required to change our password frequently, and also there are all kinds of rules about what it has to be that are, you know, frankly inconvenient. But it's important because of the data we have.

Now you might make a judgment at home that what's at risk is less and the attractiveness of stealing it is less, and therefore you might be a little bit more moderate. I do think it's important for people to be realistic. If you set too high a bar, then it's not going be honored. And that's part of the judgment here is, it's managing the risk to the appropriate level of consequence.

Question: Secretary Chertoff, this is Jeff Stein from Congressional Quarterly. Nice to see you again. I ran into a former top cyber security official in the Clinton Administration, and I asked him about Chinese -- it's well reported -- Chinese penetration of American government computer systems, and I said how do you get them out of there? And he said, semi-seriously, you'd have to shut down the whole system for two days and reboot.

My two-part question is, what is the status of Chinese penetration of government networks that you know about? And two, what do you think about that comment?

Secretary Chertoff: Well, I don't think I can get into a specific discussion about individual penetration by particular countries. I don't think you would need to reboot, but I do think a part of the cyber strategy obviously is protecting not only government networks in general but classified networks. And that, depending on the nature of the network, it's either DOD takes the lead in that or will be taking the lead in that.

And there are capabilities we have that would address the issue of sophisticated people entering the network. People enter the network or entities enter the network for different reasons. Some do to steal information. Some do to potentially deny service. So you have to configure your defenses based upon the particular concern.

You know, one of the issues people forget is, one of the great vulnerabilities is they're traveling with laptops to foreign countries. They're traveling with BlackBerries to foreign countries. A lot of these are wireless. You know, this is maybe not a personal view here. I think that sometimes there's a low tech solution to the problem, which is maybe you just don't necessarily take all of your electronics everywhere around the world. Maybe you have a travel electronics and non-travel electronics.

I mean, at some level -- that's why I want to emphasize it -- there's not going to be a magic bullet that's going to solve this. There's going to be a series of appropriate measures. Different things will suit different circumstances, but I think that's why this is -- it's a very complicated area, to be honest with you, and it's going to take work to fully deploy it. But the short answer, I don't think we have to reboot in order to deal with the issue of penetration, but we are very actively developing important tools that will protect us.

Question: Just one quick follow-up. Are you experiencing now these ways of attack that we've seen in the past at DHS?

Secretary Chertoff: You know, we've -- from time to time, we've been attacked, others have been attacked, private sector people have been attacked. I remember years ago I was out in Silicon Valley and someone showed me, one of the private companies, showed me they were under constant attack, literally, you know, hundreds of attacks a day, maybe thousands, many of them low-level things, hackers, stuff that's just nuisance. But then you'd get more sophisticated ones, too. And I think this has touched, you know, pretty much, you know, every sophisticated user at some point or another.

Question: Jena McNeill with the Heritage Foundation. I was wondering what you thought should be the top priority short-term for cyber security of government systems.

Secretary Chertoff: Well, what we're going do in the short term is we need to reduce the number of Internet access connections because it's harder to control 8,000 than to control 800 or 80. And then we need to deploy Einstein 2.0, and we're testing it now.

We also -- each of the departments and agencies need to make sure they meet a minimum standard in terms of their own security capabilities. You know, some departments stand watch 24/7. There's always someone available if there's attack that can immediately react. Some may not. Some may work, you know, business hours. Some may not have the same capabilities. So that's got to be a general upgrade across the system. That's the first priority, and that's something which I think is our short term.

But I also think that we have to be able to do more than one thing at the same time. And we are reaching out to the private sector actively to get them to think about what they need to do, and to also talk about how do we use some of the capabilities that we have and make it available to them in a way that doesn't compromise classified information but that gives them the benefit of some of the stuff that the government's been able to take advantage of.

Question: Well, to follow up on that, has the private sector been able to also give the best practices back to the government?

Secretary Chertoff: Yeah. And they do. I mean, the private sector, particularly the firms interested in this, are looking, for example, at how do you validate or standardize software and hardware? How do make sure you're not buying software that's corrupted in some way and is going to become a problem for you?

So they're doing a lot of that on their own. Of course, they're doing a lot with respect to sophisticated, you know, firewalls and things of that sort. And we do work very closely with major players in the private sector who are doing a lot of this cutting-edge stuff. So there's a lot of cross-pollination, and that's good, because this is not something the government can dominate.

Question: [Julian Sanchez from ArsTechnica] There was a report in the spring by the IEEE on surveillance architecture as security risk. An example they cited very prominently is one in Greece a few years back when the wiretapping architecture built into the national cell network was taken over by hostile parties.

And then just yesterday, there was a National Academy of Sciences report on behavior analysis and sort of data aggregation for terrorist profiling that faulted some of the -- I guess if there were set procedures in place to determine the effectiveness relative to the potential of exposure risk created by again, sort of that sort of data aggregation.

And I'm just wondering if part of the decision process when you're deciding what kind of data collection to do involves trading off the sort of actionable intelligence produced against the -- in a sense the security risk created by that kind of collection.

Secretary Chertoff: Well, the short answer to that is yes. Now let me just distinguish between several things which get confused. Because the word "data mining" is an imprecise word, and people mean different things.

I think -- I didn't read the NAS study, which I think goes back to 2005 when it was kicked off. Data mining I think in the classic sense of the word means trying to take behavioral characteristics in general and then extrapolate from that how an individual who exhibits those characteristics, how likely they are to have certain propensities. So when you get on Amazon.com and you buy three books and they tell you you're probably going to like this book, they've looked at everybody who's bought that book and they've made some extrapolations.

That is a pretty narrow band of what is often being done. It shouldn't be confused with another kind of data collection, which is if I see you have made 25 phone calls to Khalid Sheikh Mohammed's house back in Pakistan, that's a pattern, but that's not based on my behavioral analysis. That's based upon my having a specific link. And there's a tendency in the press to confuse those two.

Likewise, behavioral analysis that's individualized, like I see you behaving in way that is suspicious, that's not data mining. That's individualized analysis. I want to separate those three things out.

I would say in general, yeah, of course you always want to see the tradeoff between whether you're creating greater vulnerability or lesser vulnerability, and that's why, you know, we've talked about -- this is where the architecture matters. We've talked about the question of should you have, you know, one place where you collect all the data or should you distribute it in different places so you'd have to pulse different places? And it might be in the long run, the best way to protect data is to house it in different databases and be able to pulse the databases to get a validation up/down, which is sometimes called the ping system, as opposed to having it all pulled together in a database.

The more information you have in a single database, the greater the obligation you have to protect that. So, for that reason, you want to make sure that in the most sensitive and important databases, you have the most robust protections, and that's certainly true of the government. And I do think it's a fair point to ask, you know, whenever you build a database, what is the most secure way we could build it? What is the way that would minimize the loss of data, and, you know, how much can we minimize the loss of data risk and still have the benefit of being able to use the system?

So, I mean, I think these are all fair questions. What I get -- sometimes is troubling is though that there's a tendency to mix totally different types of systems, which are really -- is a bad mistake.

Question: [Jonah Czerwinski, HLS Watch] So, I'd like to go back to the governance issues we were talking about toward the beginning and the ways you were describing the interagency coordination, which -- as well as the coordination with the private sector.

So, the division of labor seems to make a lot of sense to me. DHS does the defensive front line kind of work. Intelligence community does its part, and DOD does its part. The private sector has a lot to offer, but also has a lot to gain.

Both of those areas require some kind of real-time decision-making process wherein the interagency part, someone is in charge of saying actually, that's a DHS role. Could you tell us more about that? And then on the private sector part, you mentioned the critical infrastructure consultative mechanism with the private sector. Are there more of those? And maybe you could speak to that.

Secretary Chertoff: In terms of how we do in the government operationally, that's real time. I mean, policy is not going to -- is rarely going to be real time. So operationally, the concept of the Cyber Security Center is, it is the -- actually, there's physical co-location ultimately, as well as virtual co-location of the major operating centers at DOD, the intel community, Department of Justice, DHS. And this is the area where -- it's like when the fly ball comes up and somebody says that's yours.

That's where this gets deconflicted, and that's supposed to be a real -- that's going to be a real time thing. It's literally, you know, with people either physically co-located and then a large group virtually co-located with what I call a deconfliction mechanism. In other words, you got it, you got it, you got it, but not a command and control mechanism. Once you have it, you execute under your orders.

In terms of the private sector, we have -- the acronym is CPAC. Now I wish I could remember. It's Critical Infrastructure something something Committee.

Moderator: Advisory.

Secretary Chertoff: Yeah, Advisory Committee. It basically works off of our 18 sector coordinating councils and government coordinating councils we have in the -- under our national infrastructure protection plan. That's been working for years now. People like that. They know how that works.

There's an executive committee consisting of DHS, DOD and DNI, and some of the CEOs who basically work to manage this process. And this is where we interface with the private sector. And the idea is you go -- let's say to the electricity people. And you say, what are your vulnerabilities? Let's talk about how we can help you manage.

Now some of them are not going to require a high tech issue. I mean, some of it may be building redundancy into the system or resiliency against physical damage or attack. But to the extent that they're concerned about someone infiltrating their IT control systems, that's an area where we can say to them, okay, we can give you some best practices. We might be able to give you the benefit of some of what we are capable of doing in terms of detection and blocking if you want it.

And I want to emphasize if you want it, because I would not want to mandate our blocking mechanisms on the private sector. I would want the private sector to say, the electricity people to say, you know, we want to have stuff that comes through our sensitive control systems go through a blocking mechanism and help us construct that. That's fine. They want to do it. They've made the choice. That's great.

That's how I see this working. In some areas there might actually be comparatively low risk of Internet attacks, and they might not be interested in having us work on that element. They might be interested in something else. But to me this is an outgrowth of what's actually been a quite successful model for dealing with infrastructure protection by bringing together the community and the government to say, what do you need, what can we bring you to the table, and what do you want us to with it?

Moderator: Guys, we can take one final question.

Question: [Jeff Stein, CQ] Just an aside on that, do you mandate controls, security controls on DHS contractors, however?

Secretary Chertoff: Yeah. If you're going to be working within our system, then our data, you have -- we set the parameters and standards for control. Now if you have other stuff to do it on your own, that's your business. But if it's going to be a threat to us, you've got to live up to our standard.

Moderator: Last one. Real quick.

Question: [Jeff Fox, Consumer Reports] I'm wondering -- there's going to be a new administration coming in within a few weeks --

Secretary Chertoff: Not a few weeks.

Question: Well, 12 or whatever. Well, they're going to be preparing in a few weeks --

Secretary Chertoff: Yeah. That's right.

Question: -- once they know. What is the Department doing to prepare for transition to a new administration?

Secretary Chertoff: Well, we're doing a lot. In this particular area, you know, we've done a lot of outreach in general in the community, and I think that involves discussions with people who are probably going to wind up being active no matter who the president is going to be.

I hope that -- you know, we put together a very comprehensive briefing we've done for the Hill, we've done for the private sector. I sat through a version of it yesterday, frankly, and I would encourage at the earliest possible opportunity, even before the election, people who might be serving in the administration or being part of the transition, to sit through that briefing, to see what's been done. A lot's been done, but there's no question it has to be followed through.

And this has been really a bipartisan effort. We've had, you know, both Republicans and Democrats working on this, because it affects all of us.

And so, yes, it's important to get briefed. Some of it will require people to get high-level clearances, but once they get those clearances, and I understand that some of that is being worked now through --

Question: So you're offering that to --

Secretary Chertoff: Yeah.

Question: -- staffers on the new administration?

Secretary Chertoff: Yes, just got to get a clearance.

Moderator: Thanks, guys. I'm sorry. Got to cut it off for now. Appreciate everybody's time.

Secretary Chertoff: All right. Thanks, guys.

###

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