

**Remarks of The Honorable Michael Chertoff
Secretary, U.S. Department of Homeland Security**

Cyber Strategic Inquiry

Enabling Change Through a Megacommunity Strategic Simulation

Washington, D.C.

December 18, 2008



General (Ret.) Chuck Boyd

Well, it's my distinct pleasure at this point and with great timing, I think, to introduce our next speaker. On February 15, 2005, Judge Michael Chertoff was unanimously confirmed by the Senate and sworn in as the second Secretary of the Department of Homeland Security. Formerly served as United States Circuit Judge for the Third Circuit Court of Appeals and previously served as Assistant Attorney General for the Criminal Division at the Department of Justice.

As Assistant Attorney General, he oversaw the investigation of the 9/11 terrorist attacks. He also formed the Enron task force, which produced more than 20 convictions, including those of CEO Jeffrey Skilling and Ken Lay. And before joining the George W. Bush administration, Chertoff served as special counsel for the U.S. Senate Whitewater committee. And spent more than a decade as a federal prosecutor in New Jersey and New York, where he investigated and personally prosecuted significant cases of political corruption, organized crime and corporate fraud, including the Mafia Commission case, in which the leaders of La Cosa Nostra were convicted and sentenced for directing the American Mafia.

If there are any people in this audience with criminal backgrounds or inclinations, you might want to head out the back way before he finishes speaking.

Secretary Chertoff graduated magna cum laude from Harvard College in 1975 and magna cum laude from Harvard Law in 1978. From '79 to '80, he served as a clerk to Supreme Court Justice William Brennan, Jr.

Mr. Secretary, we are extremely pleased and honored to have you with us today.

Secretary Chertoff

General Boyd, thank you, you've done a magnificent job with this organization which has been a real leader in promoting national security in the private sector. And I appreciate the opportunity to talk to you all here. And I'd like to express my gratitude to you all for attending, because I think it's indicative of how seriously you all take this issue of cybersecurity.

One of the challenges with cybersecurity is that it is not by any means exclusively a federal or even a governmental responsibility. It is a ... it is a shared responsibility. It's a responsibility which is held by the private sector, by people who run critical infrastructure and manage our key resources. And, as a consequence, the model for dealing with cybersecurity is to my view very different than the command and control way in which we deal with other kinds of security issues in the real world.

So what I'd like to do is talk to you a little bit today about what we are doing, both at the Department of Homeland Security and across the federal government as part of a new National Cybersecurity Initiative which was mandated by the President early this year.

And I'd like to begin by talking about the fact that, quite remarkably, the President has had personal involvement in launching this initiative. He was briefed late last year about some of what was going on in the area of cybersecurity threats and what we thought we could do in forging a partnership at the federal level between the national intelligence community, the defense community and the homeland security community. Many of you know that, historically, there was a kind of a radical division between what went on in the intelligence world and the civilian world and a reluctance on the part of the intelligence world and the national defense world to get too involved in the civilian space for fear that it might trigger judicial requirements or other kinds of liability or legal obligations that would ultimately impede the ability of the national security elements to do their job.

But when we spoke to the President, we came at with the spirit that we thought that we had a lot more we could do in partnership in a way that wouldn't compromise the security and the confidentiality of what's done in the national security world, but would allow us to leverage that capability in order to make the civilian domain much, much safer than it is both at a government level and at a private level.

And the President immediately understood the importance of this and has been personally engaged in driving forward on this strategy; even in the last week, we've had extensive briefing of him, because he's very, very concerned about making sure this vulnerability is adequately reduced and protected in the same way that he's been obviously concerned about making sure that he maintains our security in the physical world against the kinds of attacks that we've seen most recently in Mumbai.

Now, of course cyber threats, although they're different, they don't necessarily come accompanied with explosions and dramatic fireworks, we all know the damage that can ensue from a cyber attack can be comparable in scope to that of a devastating physical attack, with respect to potentially loss of life and certainly economic impact.

And we know that the challenges to our cybersecurity have grown in the last few years. In the last couple of years, we've seen Estonia the subject of a very significant attack by

people who were sympathetic to what they saw as the Russian side of a dispute between Russia and Estonia. And, when Georgia came into armed conflict with Russia, it was preceded by a cyberattack by people who shall we say were sympathetic to the Russian side of that dispute. And you might say that the cyberattack was part of preparing the battlefield.

I think increasingly we will see that accompanying traditional, physical security threats in the national security arena, there will be cybersecurity softening or follow-on designed to degrade command and control.

But the cybersecurity threat isn't only one that occurs at the level of traditional nation-states and traditional conflicts. It occurs with respect to terrorism, where we know that a cyber terrorist attack could have a potentially very, very serious impact on the safety and wellbeing of our citizens. And even common criminals have done an enormous amount of damage using the cyber system to exploit our vulnerabilities in order to make money. Earlier this summer, I announced that the Secret Service had successfully concluded probably the largest investigation and prosecution of identity theft conducted with information captured over the Internet in American history. The group that was brought down by this Secret Service-led investigation stole 40 million credit card numbers from retail companies by tapping into their wireless systems and essentially capturing the numbers which could then be used in order to simply steal money.

So it's indicative of the fact that the cyber threat is not only for those who want to attack us from a national security or terrorism standpoint, but also those who merely want to do what Willie Sutton did when he robbed banks, which is go where the money is.

So as we look at this threat, which is clearly only intensifying over time, the question has to arise what is our systematic strategy for dealing with reducing, if not eliminating, cybersecurity problems? And I'd begin by defining the problem as falling into three categories.

First is the danger that someone is going to steal information from us, whether it's financial information, whether it's credit card numbers, whether it's information about what our diplomatic or business plans are or, of course, if you can penetrate into classified networks, you can get very, very sensitive kinds of military information.

But there are two other kinds of cyber threats we have to be concerned about. One is the possibility of a threat that would degrade or destroy our ability to actually engage in activities over the Internet. Attacks that are denial of service-focused, that flood a system or bring a system down. And, if you imagine this kind of attack occurring with respect to our air traffic system or any other complex system that is managed through the Internet, you understand the potential consequences we could face if that were successful.

And then the third kind of problem, which is a little similar to denial of services, corruption of the process. Not an attack that necessarily destroys a system, but that simply corrupts it or changes it in a way that makes it unusable and undermines confidence and trust. And here, although it hasn't happened to my knowledge, imagine a circumstance where a terrorist attacked our financial system and simply altered the data in a way that left people with a lack of confidence that they could get accurate information or access to their assets. We've seen what a crisis of confidence can do in our financial system over the last six months and that was essentially an accounting problem and a problem with derivatives. Imagine if the actual information flow that is the underpinning of a financial system were to become compromised and thrown into question.

So when you consider these three major threat vectors, you understand how critical it is that we take a systematic and strategic approach to dealing with the issue of cyber threats.

Now, the way we've approached it sitting down with our partners in the federal government is to focus our cyber initiative from a strategic standpoint on three main pillars. The first is establishing front lines of defense, which basically means reducing our current vulnerabilities and preventing intrusions. That's essentially perimeter defense of the border, so to speak.

The second is recognizing that, while the most publicized threats to our cyber networks are people hacking in over the Internet, those are not the only threats and we have to defend against the full spectrum of threats by having a serious look at our counterintelligence approach—in other words, how do we make sure that people aren't compromising our system from within? And also by looking at the security of the supply chain. Because some of the threats that we're experiencing to the Internet don't come by people coming in over the network, they come by people corrupting the hardware and software that is, of course, that architecture through which the Internet operates.

To give you an example, a couple of months ago there was a story in *The Wall Street Journal* about money that, financial information that was being exported from ATMs in Europe to locations in South Asia. This was not an example of people hacking in over the Internet to get into the system. It was a device that was placed in the chips, that was actually put into the hardware of the ATM systems and acted like a beacon. And, when it was turned on, periodically, let's say once a day, it sent information back to its home port over the Internet. But it had been placed in the hardware before it was installed. So the compromise of the supply chain becomes every bit as important as a potential threat as someone simply coming in over the Internet itself.

So, having laid out these three pillars, let me give you a little bit of a sense of how we actually see the strategy moving forward in each of the pillars I've described. First, how do we establish front lines of defense? Well, from the standpoint of the civilian domains and the government—because the military domains take care of themselves, that's a separate responsibility—we have to recognize the vulnerability that exists when you have multiple federal agencies with literally thousands of connections to the Internet, varying degrees of capability in terms of watching, warning in their agency operation centers and a lot of ways in which someone might intrude into the network of a civilian network through the weakest link and then, once inside, can move around and essentially attack from within.

It becomes clear when you think of that architectural problem that the right answer to respect to beginning to protect our government domains is to reduce the number of external points of access to the networks so we can patrol a limited number much more effectively, upgrading our U.S. cert capability so that we go from the ability to do forensics after an attack and determine that we had an attack and take remedial measures to a real-time capability to detect in order to warn in real time and ultimately to the ability to detect and block in real time, which is the ability essentially to shoot down the enemy before the enemy reaches its target.

As you consider what we face in the civilian domain, you realize that only if we take these steps can we begin to move out of our current system where we are hostages to the weakest link in the network into a system where we have a high confidence level that we can monitor what comes into federal domains and make sure we can stop a problem before it actually comes to fruition.

A big part of this is what we're calling doing with our system called Einstein. Einstein, in its current form, is what I describe as CSI: Miami in the Internet. A crime's been committed. The intrusion's occurred. We become aware of it either because the victim becomes aware, because we've seen an anomaly after the fact and we come and we look to see what we can learn about what happened and how we can remediate.

That's not the best way to deal with this. So we've gone to Einstein 2.0, which are currently deploying at the Department of Homeland Security and look to be deploying in other places around the government in short order. What this does is it detects in real time. And it detects in real time using certain capabilities to look at either the characteristics of the flow or some of what might be in the packets in order to see malicious code as it's coming into the network. In other words, we have to teach the civilian agencies to be mindful about the security of the people inside their own agencies who have access to the Internet. Some of this involves, obviously, traditional counterintelligence, making sure people are properly cleared and, if they have access to sensitive networks, that we're checking to make sure they're not getting compromised.

But some of it is building an internal architecture that does things like make sure that people only have access to elements of the system that they should be entitled to have access to. Or having audit trails. Or having rules, enforceable rules with respect to the kinds of outside devices you can bring into the system and put into the system. Because only if agencies take that seriously can we prevent people from literally walking in the front door and stealing what we're trying to lock down as we protect the system on the back door.

And, likewise, on the global supply chain. In a world in which we increasingly see the ingredients of our software and our hardware generated from all over the globe, including in countries which are not necessarily synchronized with us in terms of worldview, if I could put it that way, we've got to have the capability to determine whether the software and the hardware we are using in sensitive systems poses a threat. And that's going to be something which I know the private sector's working on and we need to be able to encourage both in terms of standard- setting and research and perhaps even to some degree within our own domain mandates.

Finally, the third pillar is shaping the future environment, which involves helping to foster increased education and training in this field of security, which I think we need to build a cadre of smart young people who get into this field. It means research and development, particularly for that kind of technology that would give us a leap ahead in terms of achieving the kinds of results I've talked about.

And maybe most important—and this is what I want to spend the balance of my remarks on—cooperation with the private sector, because I come back to that initial point of recognizing that we don't own most of the assets and we don't employ most of the people who are in the network. And therefore we're going to have to work with others in order to make this happen.

I want to begin by saying that I'm very sensitive to the fact that the culture of the Internet, as well as the actual architecture is one which does not lend itself to government regulation and mandates. I think it would be a very dangerous road to go down to have a lot of effort to have the government lay a heavy hand on the Internet. There are countries in the world that do that and they do it for nefarious purposes. I think our model here has to be different. It has to be a model where we invite cooperation, we facilitate cooperation, we are willing to provide capability to those who want us to provide that capability, but we don't make you do it. And, if someone doesn't want to have the government involved and they want to live outside of any kind of government assistance or cooperation, I don't know that we would necessarily be wise to try to make them do it.

Now, we might have certain requirements about people who deal with us and people who contract with us, but I think the sensitivity to the civil liberties point is most acute when you get into any question of how you deal with the Internet.

So, what are we doing? Well, the first thing we're doing is we're working with the private sector using some traditional pathways that we have already established and are well-established for dealing with infrastructure protection across the board. As you know, we have sector coordinating councils and government coordinating councils, including in the area of IT and communications, but also financial services, power generation, a whole host of areas—nuclear power plants—where we have traditional, accepted and lawfully ratified ways to communicate with each other about things like best practices, establishing information flow and a common operational picture about threats, capabilities that allow us to leverage private investments and work with the private sector when there is a problem, whether it's a physical problem or a virtual problem to help them solve that.

Using these existing pathways, which are well-recognized in the law, and our National Infrastructure Protection Plan, DHS is using, is employing the cyber initiative or executing the cyber initiative through the very same mechanisms, these coordinating councils. We are using the coordinating councils to discuss and come to consensus on policy issues and we're using our information sharing and analysis centers to share information from an operational standpoint when we have events going on that require sharing.

DHS, in collaboration with a number of our partners, have established a cross-sector Cybersecurity Working Group. This group meets monthly and includes industry and government representatives from all of our 18 critical infrastructure and key resource sectors. The idea here is to exchange information on vulnerabilities and strategies for mitigation, have briefings in both directions about what we are seeing and what we're concerned about. And also to participate in specific projects, including projects to develop metrics to see how we're doing in cybersecurity, an incentive study and some other pilots about information sharing.

In particular, we're focused on chemical, IT and banking & finance sectors, because we know those are sectors where there's a particular concern about the collateral consequences of a cyber attack.

Additionally, besides this process of using the coordinating councils, we have required from each of the sectors a comprehensive risk assessment under the National Infrastructure Protection Plan. What this will allow us to do is identify and assess our risks with a particular attention to the needs of these sectors of the economy, which are very, very different.

The information technology sector has developed an IT sector risk assessment methodology, which assesses risk to functions of the sector as a whole and they've nearly completed a baseline risk assessment which will help us more precisely target, on a tactical level, our protected programs and our R&D.

We have a whole host of other working groups that are designed to make sure we are identifying vulnerabilities, we are focusing on areas where we might supply research and development if industry doesn't have the business case to do it on its own. And, at a classified level, we are working with the IT sector to have a Threat Intelligence Coordination Working Group that allows us to use classified [CIVITS] and conference calls to exchange information about what we are seeing.

Obviously, this is a work in progress, but it is one which builds upon a shared relationship of trust and experience which we have seen work in the physical realm. And one of the reasons we have to work across the entire domain of our relationships with the private sector is because the needs of each sector differ in terms of what their concerns are from a cybersecurity standpoint.

The financial sector, for example, may be very concerned about the integrity of its data; they happened to be quite well advanced in terms of their own cybersecurity and so they may be very focused in issues, for example, on supply chain or how to protect against network intrusions. But other sectors may be actually concerned about physical vulnerabilities to their servers or to their IT systems and so they may want to integrate cybersecurity with physical security.

One of the reasons I think it's so important to keep the Cyber Initiative within the same framework as our physical initiatives is because, quite frankly, I don't see the radical division between the two. I think the two are deeply integrated at every level and the tendency to stovepipe, which is something we have fought traditionally, certainly over the last 8 years in dealing with threats—the danger of stovepiping is particularly acute if we have the people who are focused on cyber divorced from the people who are focused on physical security. More often than not, the two are going to go hand-in-hand.

Finally, let me say again, I think it's going to be important, as we move along in this process to continue to talk publicly about what we're doing to protect privacy. I know in terms of what we deploy in the government domain, we are very sensitive to making sure that our presence is consistent with all the requirements of the privacy laws and, of course, the Constitution. As we engage with the private sector, we need to make sure that our enthusiasm for getting us into that space does not put us in the position where we suddenly appear to be uninvited guests. And that's why I'm really emphatic about the

need to not make this a mandatory system, but rather a system where we create opportunities for people.

I actually think most people in the private sector will take those opportunities and will accept our invitation. But I also know if we try to make it something that we push onto people, the backlash we are going to see will dwarf some of the controversies that we've seen with respect to what we've done in the communications field over the last 8 years, so here's an area where my own view is careful movement and attentiveness to sensitivities is very, very important as we build and implement our strategy.

Let me conclude by saying we know we're entering a transition. I'm sure this is going to be a major area of focus of the new administration and we obviously want to work with them to help them get the benefit of what we've done and whatever advice they seek from us.

I do think that we have a partnership in place now with the Department of Defense and the intelligence community which is beginning to work very well in terms of how we manage cyberspace. It is what I would call a federated system. For those of you who work in the world of the Internet, the idea of a federated system and shares space makes a lot of sense. The culture of the Internet is a network culture. It is a culture of not command and control, but collaboration and cooperation. And the way we have set up the architecture of our current system, with DoD maintaining its distinct responsibilities, the intelligence community maintaining its responsibilities and DHS and DoJ doing its piece in the civilian space, I think that works well. I think it preserves existing authorities, which have been separated over time, frankly, to protect our civil liberties. And yet it allows us to exchange and work in a cooperative way that gets the benefit of what DoD and the intelligence community does and yet does not make them responsible for what we do in a civilian space.

I emphasize this because sometimes there's an urge, I get asked, "Well, shouldn't there be on person in charge? Shouldn't there be one agency in charge of everything?" And I must tell you that, having been part of debates about national security not only over the last 8 years but over the last 20 years going back to when I was a U.S. attorney, I think you ought to think, people ought to think very carefully before they do that. A system where one agency sits over everything, military and civilian, is not usually one that has been regarded favorably the American public. And it is one that is fraught with peril by putting all your eggs in one basket.

So I certainly will urge those who are looking at what we are doing now to take a careful look and see how it works before suggesting major surgery.

This strategy's been a long time coming. It's been a long time coming because the Internet has been the hardest issue philosophically to grapple with from a security standpoint, precisely because it is so widely distributed and its culture is so antithetical to the traditional, mandatory command and control way which we deal with security issues. But the fact that it's a hard problem doesn't mean it's a problem we ought to avoid. And that's why I'm pleased that the President mandated that we step up and get this job underway and I think we've done an awful lot in a relatively short period of time, as government work goes. And while there's much more to be done, I think we've teed it up so the next administration has some momentum and I will encourage them in any way I can to continue moving forward.

Thank you very much.

I'll be willing to take a few questions, if you just tell me who you are.

Chris Kelly

Chris Kelly from Booz Allen, thanks for your remarks, Secretary. Today and yesterday, we saw the exercise of some of the partnerships that you talked about. Working together, working on problems and things like that. One of the things we did see, though, was a potential gap in engagement with the American public. Could you talk a little bit about your views about where you think engagement with the American public needs to be and how the Department fits in with that?

Secretary Chertoff

Well, I think you're absolutely right, we need to get the American public engaged in this, partly because, of course, they will have to decide themselves how much they want to participate in this.

We have tried to talk about this a lot, I've done a lot of getting out on the road and talking about it. Although, I have to confess, probably largely to industry groups or people who come to this process with a preexisting interest. And part of what I confess I'm a little concerned about is we do find that a lot of this information is classified and it's hard to talk about. I think we need to take a hard look at whether we can declassify more of what we're talking about. I am very acutely aware of the need to protect sources and methods, but I also think sometimes we become so overprotective that we don't recognize there's a cost involved in being too obscure. Because if we're too obscure, we appear to be mysterious and I think mystery is actually the opposite of what we need to do.

So I'd like to suggest one of the things that we do as we go forward is take a hard look at whether we can talk more about what it is we're doing openly and also in a way that's more clearly explicable to the American public. And this is an area where the private sector, working through your network, can do an awful lot in order to carry that message

forward. Because in the end, you know, I've been through countless security measures where someone winds up mischaracterizing what happens and then you're behind the 8-ball because we're explaining that we're really not Big Brother.

And a classic example before my time was a search engine, I think it was called Carnivore, which the FBI came up with. And I think it made a lot of sense, but the word "carnivore" was the absolute wrong thing to have in that program.

So getting out there ahead of the misinformation is going to be critical in terms of making this thing work.

Demetri, yeah.

Demetri Sevastopulo

Just along, in the same vein, one of the things that we noticed yesterday and today participating in this game is there doesn't seem to be a kind of a strategic communications crisis plan for cyber attack or cyber crisis. Does the government have one of those and what would you do today if you went back to your office and all of a sudden everything was falling apart?

Secretary Chertoff

Well, I think you're quite right, we need to have a plan tailored for a cyber crisis. Now, we do have crisis communications plans for the whole range of crises and, obviously, we would deploy that immediately. The key would be to be able to tailor it specifically to the cyber environment. And that would require us to do a couple of things. We'd have to first of all have a clear awareness of exactly what the dimension of the threat was and therefore what people needed to worry about. And that's why developing that plan is critically dependent on having, at a minimum, a real-time intrusion detection and characterization capability, so you can talk intelligently about what it is.

And we'd also need to figure out, again, this goes back to the earlier point, how much we can talk about this without getting into an area that's classified.

So I think the short answer is we would probably take the existing plans and adapt them—and some of the basic principles I think are applicable no matter what you do, which is have authoritative people speaking about something, have regular briefings, make it simple and be able to explain it in terms that are meaningful to the American people.

I do think that we have work to do in figuring out how to tailor something specific for cyber security in the same way that we've done it for natural disasters or terrorist attacks or things of that sort.

Frank Plantan

I'm Frank Plantan with the University of Pennsylvania. Can you take what you've said today and think a little bit broadly—globally—how the Internet is part of the global commons now. And what are the special challenges of cooperation you face globally and who are going to be our partners in engineering a security regime, a cybersecurity regime that's global and not just domestic?

Secretary Chertoff

That's a great question. We—I want to answer it at two levels. One is that we traditionally dealt with this in a law enforcement way. We discovered that, when I was at the criminal division, one of my sections, one of my units was the computer crime section and so we had to work with other countries when there were cyber attacks to see that they took steps against the people who were perpetrating the attacks elsewhere. Now, of course, there's always a characterization issue, you have to know where the attack's coming from and, as you know, with botnets and other kinds of tools, it's possible to very effectively mask where things are coming from. But even if we know what that is, we need to get the other country to agree and have the capability to take legal steps. And that's been challenging. I know there's a U.N. convention on this that we tried to sign up people to and we had, if I recall correctly, a kind of a network of 24/7 watch and warning standards that would allow us to work around the world.

But there's a larger issue looming out there which is a doctrinal issue. Which is, what if we do if we actually have not just criminals attacking, but we actually have terrorists or a nation-state attacking us? Is this an act of war? And what does that mean in terms of our doctrine to how we respond to an attack?

We know that if someone flies, shoots missiles at us, they're going to get a certain kind of response. What happens if it comes over the Internet, if it's a terrorist group? If it's a terrorist group sitting in a safe haven. If it's a nation-state enabling the terrorist group? If it's a nation-state itself. And what is the level of proof we're going to need? And what are the steps we're going to take to respond?

That is the kind of doctrinal strategy that we haven't put together yet. One of the things that has been talked about in a comprehensive cybersecurity strategy is to sit down and put together some deep thought about the doctrine with respect to cyber attacks in the same way that we developed doctrine 50 years ago when we were entering the nuclear age and we had to suddenly conceive of a new way of thinking of attacks.

This opens up interesting legal questions in an international domain about what the responsibility of a country is to make sure it doesn't become a launching pad for cyber attacks against another country. Do we have to move beyond voluntary, cajoling people

to join a convention into something a little bit more coercive from the international community?

So I think that, because we're entering a world which in some ways parallels the physical world but in many ways is different, we just haven't done the thinking. And partly, you know, honestly, it's because it's hard. Because when you start to think about how do I deal with a cyber attack from another country, what do I have to prove? What do I have to show? Who do I have to prove it to? What am I prepared to do? It gets pretty uncomfortable.

But my takeaway from eight years of doing this stuff or more is, the fact that a problem is hard doesn't mean it shouldn't be addressed, it just means we have to kind of bear down and address it with more energy and maybe more speed than we've done up to now.

So that's my—maybe long-winded—that's my view of what we need to do, taking note of the global character of the challenge that we face over the Internet.

General Boyd

One more, Mr. Secretary? And the last question?

Craig Piper

Craig Piper with the *Washington Internet Daily*. I was wondering if you had maybe an estimate when Einstein 3 might go live. I know you're just implementing Einstein 2. And also how you think the organization may change going forward in the next administration, especially the role of the Assistant Secretary for Cybersecurity & Communications and some of the other groups?

Secretary Chertoff

Well, in terms of the—I'm sorry, what was the first question? I got the second one. Oh, we're going to begin a live exercise of Einstein 3 I think within the next six months. Probably sooner rather than later.

I can't speak organizationally for what the next secretary's going to do or the next administration's going to do. As I said, my belief is that, although—and I know Congressman Langevin is here, I know that the CIS report suggests that some kind of White House oversight—and I think there's value to that—By the way, we have that now, I should make it clear, the White House has played a policymaking role—I would be hesitant to see a White House get into operational activity over the Internet. My own view is that's, for a variety of reasons, some of them legal, some of them historical, that might not be prudent.

But I'm going to leave the decision, as I have to, to the next people and, if they ask me for my advice, they have my phone number once I leave. Other than that, I will continue to urge, whatever the precise way in which the boxes are arrayed, that this get the kind of high level attention that the President has put into it in this administration and that my senior level counterparts have put into it in this administration. And I have every reason to believe that the next administration will continue to give it that intense level of focus.

Speaker

Thank you, Mr. Secretary.

Secretary Chertoff

Thank you very much.

End of speech and Q&A