The National Conversation at the Wilson Center
Cyber Gridlock: Why the Public Should Care

Jane Harman:
Good afternoon. Steve, you're here.

Steve Inskeep:
Okay.

Jane Harman:
Good afternoon.

Audience:
Good afternoon.

Jane Harman:
This is a good class, to hear about a very important subject. I'm Jane Harman, the president and CEO of the Wilson Center, and I want to welcome those here physically in the audience as well as those tuning in via C-SPAN and live webcast, all terrific tools for bringing even more people into this critically important discussion. The Wilson Center recently joined forces with NPR to create this public event series we call "The National Conversation." Our hope is that this series will provide the public with new opportunities to engage in much needed civil discourse, let me underline "civil" discourse, free from spin -- imagine that in this election season -- in the safe political space that the Wilson Center provides. New York Times reporter Scott Shane, is Scott here? I'm going to out him if he's here, maybe he's listening in. Anyway, he wrote an article last week about how cyber warfare is just beginning to emerge from the shadows for public discussion by U.S. officials. Lack of public knowledge about cyber security is, in my view, truly frightening. In the past two weeks alone, the websites of Bank of America, JP Morgan, Wells Fargo, U.S. Bank and PNC have all suffered from "denial of service" cyber-attacks, and apparently that didn't even take much effort on the part of the hackers. Does a cyber-911 need to occur before anyone starts paying attention?

When I attended the Aspen Security Forum in late July, Gen. Alexander, he'll be introduced and you'll hear from him in a moment, said we need to get the public into the conversation about cyber security. I thought that was a magnificent idea and this National Conversation is our

attempt to use the convening space of the Wilson Center to do just that. Wilson hosted John Brennan in April, who spoke publicly about guidelines for the U.S. Drone Program, and we're hoping today, in a similar fashion, to lift some of the fog over cyber, another key tool of both espionage and combat. It's easy for an issue like cyber to become polarized when the public doesn't know the facts. The facts, which will be spelled out much more clearly during today's panel discussion, are that there have been massive foreign intrusions not only into government networks but also into private networks like governments, companies, and individuals. In the Republic of Georgia, there's an election going on today, there are allegations that there have been cyber-attacks between the candidates. Investigators allegedly found 56 malware infections on five computers operated by the president's political rival. The clever virus could turn on the computer's cameras and microphones, capture story screen shots every 10 seconds and record keystrokes and passwords. Anthony, I bet that gives you chills, and I'm with you.

Some threats, like the emptying of your bank accounts or the shutting down of the power grid are easier to visualize. Others, like the online theft of intellectual property are harder to wrap our heads around. Cyber doesn't respect nation states, and that's something we need to, but aren't, thinking about. The debate, at least as I see it, is taking place at 30,000 feet and we don't have a way the public can participate, and that's all while, as Gen. Alexander said at that Aspen event, cyber-attacks in the U.S. increased 18-fold from 2009 to 2011. And the irony is that a lot of the folks who were doing this, or some of them anyway, are trying to return us to the 7th Century Caliphate by using the most modern tools. They attack us asymmetrically; we need to be thinking outside the box if we're going to repel those attacks.

I'm persuaded that one of the best uses for Wilson's platform is to bring the stakeholders into this conversation and I'm very excited about doing this today. There's a lot to talk about, including the scope of the problem, the gridlock on Capitol Hill that is preventing a careful legislative response, the limitations of executive action, and the huge consequences if we do nothing. What has to happen is for the public, including advocacy organizations like the ACLU, to agree to help solve the problem. No more time for the blame game, time now to

solve this problem. But without a debate in the public square, we won't move forward and we could easily have, I'm sure Senator Collins will tell you, a devastating attack. My hope is that, with clearer understanding of information, answers will emerge. And so, we have a terrific lineup for today's event. As I like to tell Steve Inskeep, the host of NPR's Morning Edition, he is the first male voice I hear when I wake up every morning and we've never even had a fight [laughter]. He covered deliberations over the Cyber Security Act of 2012 which is proposed by Senators Joe Lieberman and Susan Collins, and he's moderated several spectacular events here at the Wilson Center. Welcome back, Steve.

Steve Inskeep:
Thank you.

Jane Harman:
In all objectivity, Susan Collins, the ranking member of the Senate Homeland Security Committee, is one of the best legislatures who has ever served in Congress, ever. You can applaud, go ahead.

[applause]

We bonded, I think this is actually true, it's urban legend but it's true -- we bonded during intelligence reform in 2004 and I have called us ever since the bi-cameral, bi-partisan sister act. I don't always have warm and fuzzy relations with the ACLU; however -- and they have wrongly disagreed with me from time to time.

[laughter]

But in Anthony Romero, I found a man with an excellent and open mind who is ready to engage; he and I have had many discussions on this issue, and I think you're going to be impressed with the role he is playing in this panel. He survived testifying before me when I was chair of the Subcommittee on Intelligence Information Sharing and Terrorism Risk Assessment, so today should seem like a piece of cake after that. But finally, we're very privileged to have Gen. Keith Alexander, whose insights inspired today's discussion. Gen. Alexander is the director of the National Security Agency, the chief of the Central Security Service and the commander of U.S. Cyber Command. On a scale of 1 to 10, I think Gen. Alexander's

given us a three for preparedness for a cyber-attack, and he has repeatedly expressed his support for the approval of a comprehensive cyber security bill. He's extremely knowledgeable, but even more important than that, he is the rare technical person who can explain things in English. If we think we need former President Bill Clinton as the Secretary of explaining things, I think we need Gen. Alexander as the Secretary of explaining technical things like cyber. This is an issue I am passionate about, as I have told some of you. I serve on four advisory boards for this administration: the Defense Policy board, the Foreign Policy Board, the CAIA External Board and the DNI's Board, and I co-chair the Aspen Homeland Security Group with Michael Chertoff, former Secretary of DHS Michael Chertoff.

So I'm joining this panel just to make sure that everybody gets everything out, and the goal here, one more time, is to involve you in this conversation. This isn't a conversation to talk at you, this is a conversation to get you and your ideas to the forefront and to make certain that you too want to join us in solving the problem. So please welcome Steve Inskeep and a spectacular panel and welcome to many of you back to the Wilson Center.

[applause]

Steve Inskeep:
Thanks very much for a powerful introduction; I really, really appreciate it. A powerful warning as well, in fact, as you were talking, Miss Harman, I was looking at the coffee table and trying to think if we could all get under it or if it's just not large enough. So, you've laid out some strong problems there.

But I want to begin by defining the problem a little bit better, if we can, because you spoke of denial of service attacks on banks, you spoke of the possibility of a digital 911, you spoke of different possible enemies or adversaries, and I'd like to narrow that down a little bit. If we were going to try to name a central concern that the United States has or should have, what kind of attack are you most concerned about, what kind of enemy or adversary would be behind such an attack? Any of you can start. General, you could start, in fact.

Keith Alexander:

Well, I'm not going to name specific countries because I think in this environment that wouldn't be the appropriate way to handle it. But let me -- let me give you the class of attacks that I'm concerned about. I think for the last ten years, what we've seen on our networks has been essentially exploitation or the theft of intellectual property, crime, those types of events. The congresswoman pointed out over the last few weeks we've seen distributed denial of service attacks, so we're seeing the threat grow from exploitation to exploitation and disruption, and my concern is it's going to from exploitation and disruption to destruction. And what I mean by destruction is the physical destruction of computer devices on the network which would cause these networks to fail. That's my greatest concern, or, the loss of a significant amount of data that would impair our companies' ability to operate; the stock exchange or the power grid. All of that's within the realm of the possible. The consequence means that we have to work together and understand this. I think if I were to put one thing on the table, it's education. You know, on cyber, the key thing is understand what's going on in the networks. We really got to understand that so that we can all get together and come up with a solution that will solve that problem.

Steven Inskeep:
Are you suggesting that even the people who run the networks do not fully understand what is happening on their networks?

Keith Alexander:
I think the people who run the networks understand what is happening on their networks given the information they have. The problem is, they don't have all the information. Government has some, they have some, academia has some, we're not sharing. Part of the legislation is, why don't we share this data? How does government take classified information and share it with industry so that they can help identify when there's a problem and tell the government? That's part of the solution, I think, is to address this in such a way that we're transparent in our actions, and I think this really gets to some of the discussion we were having before with Anthony. I think we can solve the civil liberties and privacy concerns and the cyber security. The way to do that is transparency, it's by having all of government work together. That doesn't mean just NSA and Cyber Command, NSA, Cyber Command and

FBI; it means DHS with industry. And, we know things that they may not know and we need to share them and say, if this happens on your network you got to tell us. We don't need to be there to screen traffic, they can tell us. They see the traffic, they can say, "I saw a red car going by and you said if a red car goes by this is bad. A red car just went by, it's bad. Help." And that's where we would come in. And I think in that manner, a couple of things are on the table. One, transparency, you've got multiple organizations working together. I think you've got us working with industry, and a great part of some of the bills that are on there is the information sharing and the liability. We need those. If we don't do that, what I'm concerned about, what's going to happen and you're seeing this, it's creeping up from -- and we made that discussion a year or two ago, we said it's going to go from exploitation to disruption. We're now in disruption and you're seeing that, to destruction. And destruction could be overwriting data. It could be overwriting the basic input/output of a system and the ability for a system to turn on, which would cause a number of our systems to go down, or any one in between. I believe that's coming our way.

We have to be out in front of this for a whole host of reasons. The Defense Department's reason is we depend on critical infrastructure to do our job. We depend on the power grid. We depend on the Internet to operate.

Steve Inskeep:
Just so that we're clear on our terms, when you talk about disruption versus destruction, the attack on PNC the other day, as we understand it, was just basically flooding their computers with requests.

Keith Alexander:
That's --

Steve Inskeep:
It didn't actually -- didn't actually break through a firewall that just overloaded the system.

Keith Alexander:
That's just a disruption, you know, it's like kids in your car, they're yelling and screaming -- I have four daughters and fourteen grandchildren –- they're all in the back, they're talking, we're trying to talk, you can't get a word

through, that’s disruption, that’s a distributed denial of service attack. Now, if you give them weapons, that’s a whole different ball game.

[laughter]

We’ve not done that, not even as a test, but you can see the difference would be right now it’s is once that stops they can go about doing their job and the Internet service providers can, to a large extent, filter out part of that disruptive traffic. But it does have an impact, it does slow it down, it does impact those companies, and as a consequence, if you think of a company that makes its job on the Internet, like a stock market or Amazon or one of those, and somebody impairs the ability for them to get that, that slows down their business, that has a top line impact. If you destroy the infrastructure, that company is seriously impacted and probably going to go bankrupt.

Steve Inskeep:
Can you, and I want to bring other people into the discussion here, but first let me just ask, can you name a recent instance in which someone has moved to destruction? Actually destroyed something.

Keith Alexander:
I think there’s been some public ones on that, I think --

Male Speaker:
Aurora.

Keith Alexander:
Which One?

Male Speaker:
Aurora.

Keith Alexander:
Yep, there’s Aurora, and then there were some other ones that are out there.

Steve Inskeep:
Why don’t you explain what Aurora was.

Keith Alexander:
Well there’s -- well let me go to one that I think is more recent, which was Aramco.

Steve Inskeep:
Okay.

Keith Alexander:
It was public, and a number of their computer systems lost a lot of data; I think in the press it said 20,000 or 30,000, lost all the data on their systems. Think about a company that loses all the data on their systems. That doesn't mean you just go to backup, it's gone. And if you lose that data and that data had important information, you can never recover it. So, you'd have to back up. From our perspective, that has a significant problem. The other part, though, as you look at this and you look at the way the network operates, you know, parts of these are routers and stuff that helps traffic go through, parts of these are systems that tell you how to get from point A to point B, domain name servers. And when you start thinking about how the network is brought together, if you start to wipe out data on there, you wipe out the ability for the network to operate. That's a significant concern. That means that the calls from my kids to us won't come through because it can't -- it doesn't know how to do it. And most of that is digital today. Now I could live with that, but my wife couldn't, and so I do think we have to get out in front of it, really for the operation of our government and our country, but it also will have a significant economic impact.

Steve Inskeep:
So you named going from -- going toward destruction from disruption as being one of the major problems here. Senator Collins, when we were talking about network operators maybe not understanding everything that's going on in the networks, you nodded. You don't think that people know what's going on.

Susan Collins:
Well, there have been surveys that have shown that 40 percent of the owners and operators of core critical infrastructure, our financial networks, our water treatment plants, our transportation systems, were not hardening their computer systems sufficiently. In just the past year, over 200 examples of cyber-attacks to core critical infrastructure, are national assets, have been reported to the Department of Homeland Security, and that is only the tip of the iceberg. Undoubtedly there are many more that

have not been reported. We have found that some companies don't do some basic steps as changing the default password that comes with the industrial control systems that are used to control the networks.

Steve Inskeep:
You mean 1-2-3-4-5 is not a strong password?

Susan Collins:
It's not a good one.

[laughter]

Nor is the word, "password."

Steve Inskeep:
Oh, that's even better.

Susan Collins:
But you know, if you look at this more broadly, I think there are three areas of concern. One is the threat that it poses to our economy, because it is our economic edge; our intellectual property, our R&D that is being stolen. The general memorably has said it's the greatest transfer of wealth in history; it costs billions of dollars and millions of jobs to our country. The second, and to me the most worrisome, is the threat to our core infrastructure. Look what the storm in the Washington, D.C. area in June did to us when it wiped out the electric grid for so many people. Well, multiply that many times, if it were a deliberate cyber-attack that took out the electric grid for the entire East Coast. And the third area of concern is the threat to our privacy. The ease with which transnational criminal gangs, for example, can steal private information and have done so from numerous organizations and companies.

Steve Inskeep:
Although there's different layers of threats there, and I'm trying to figure out as a citizen which one to be more worried about. Should I actually be more worried about general intellectual property theft, that transfer of wealth? Should I be more worried about that than a digital 911 type attack?

Senator Collins:

I personally am most worried about an attack on our core critical infrastructure such as the electric grid, because that could cause a loss of life, destruction of property, a terrible impact on our economy. That cuts across everything, and to me, that is the most serious threat. But I don't in any way minimize the threat to our economy of the continual theft, particularly by China, of our intellectual property and R&D. There's one case where a company lost in 20 hours a billion dollars' worth of R&D. That has a real impact on our international competitiveness and our ability to create and preserve jobs.

Keith Alexander:
Can I --

Steve Inskeep:
Oh, go ahead please.

Keith Alexander:
Could I add to that? Because I agree 100 percent with the senator. In fact, you know, I asked our folks to look at this because I agree. Both of these are the issues that we are facing, and we can solve both. I mean, both of these are solvable. And we should put them both on the table. I think the theft of intellectual property is absolutely significant, and you think about what's going on and the way it's being taken, we can and should do everything we can to stop that. If you look at -- and so I had our folks go back, and if you go just before the iPhone came out, Apple stock was at about $70 -- $85 a share. After the iPhone 5 released, it's at $700 a share. I missed that. [laughter]

But, let's say -- now let's turn that around, let's say that Apple's intellectual property for the iPhone and iPad were stolen, think about if somebody beat them to market with some of that, what the impact would have been on their stock and on us, because that would have affected the New York -- or the -- our stock market, the NASDAQ, and when you look at that, this is just one company. Now they haven't been hit, but you look at the companies that we were -- that you were talking about, some of those have been bankrupt: DigiNotar.

Steve Inskeep:
Go on, tell the story, what happened?

Keith Alexander:
Well and so, DigiNotar was one that had certificates and they worked with Google and others, were stolen by an adversary. The certificates allow you to communicate securely between two -- say, I know that you're Google and that you can update my Chrome system and you have a certificate to come in and do that, so I accept those as verified that you're the right person coming in. Somebody stole those so that they could hijack those communications and DigiNotar went out of business in 30 days.

Steve Inskeep:
So a company that was providing secure communications had its security compromised --

Keith Alexander:
So really what happened is the faith of companies like Google in DigiNotar went down to the point where they went out of business, bankrupt. And you look, RSA, probably one of the best, no, they didn't go bankrupt. They're probably one of the best standards in the country in terms of cyber security. They had a break-in, very public, I think they handled it very well. Again, somebody wanted to steal their two factor authentication like PayPal, and so what they're doing is they're stealing this to get deeper into networks of some of these companies like Lockheed and others. And you see this going on all the time. And so it is a significant problem. And the two problems, if you put them on the table, overlap in that they both depend on malicious software to get into your system or to make something happen, and I think –-

Steve Inskeep:
Two problems meaning, intellectual property theft and actual attacks.

Keith Alexander:
And disruptive destructive attacks; the two parts that the Senator mentioned. So if you put both those on the table, the solution is information sharing.

Steve Inskeep:
Right.

Keith Alexander:
Working together in a transparent -—

Keith Alexander:
In a transparent way, and I think that was, that was where our conversation --

Steve Inskeep:
Anthony Romero, help us continue to define the problem.

Anthony Romero:
Yeah, I mean so far there's nothing with which I can disagree, and all I can do is whole heartedly endorse both the fact that Congresswoman Harman is having us have this discussion is incredibly important. And when you asked the question about what are you most concerned or afraid of, it's -- the -- when we talk about information technology and cyber security it's every aspect of our lives, from communicating with our children, to our doctors, to our banks, to our government. I mean, remember, we have electronic voting systems in part of this country. It's not far-fetched to think that they're also a key part of how the body politic works, and so --

Jane Harman:
[affirmative]

Anthony Romero:
That's why I'm just thrilled to be a part of the discussion here, especially with Senator Collins who's played such a critical role, and General Alexander. This issue requires a public debate, and if there's one thing I fault the legacy of where we've been before on intelligence and security, especially in the years of President Bush, has been we didn't have these fora. We didn't have these debates. They were done often in secret without C-SPAN covering it, and without the public debating it. And so we are all the better for having this discussion, and all I can say is personally, it's every aspect of our life is affected by this. And protecting the infrastructure of how it affects our everyday lives is an obligation that only the government can fulfill. It is not a private sector obligation. It can't be a group -- a non-profit organization such as my own that can fulfill that obligation. It is the government's obligation, and we have to help them get there. And I will just say, from my point of view, I'm the head of the American Civil Liberties Union, I'm also a CEO of a corporation. We have $350 million in assets. We have 900 employees nationwide. I

have a membership list of 550,000 members that are my bread and butter. I mail to them. I get hacked all the time. People are always attacking us. Now I'm sure no one in this room.

Jane Harman:
[laughs]

Anthony Romero:
But there are a number of individuals who may disagree with our substantive points of view, and they shut our system down, they try to get into my membership file, they try to get into my bank data. And so these are concerns which I very much share as an individual. Not just as an American who wants to be able to call my mother, and make sure her doctor's appointment went well, because the wrath of God will be great if I don't make that phone call when she expects it.

[laughter]

But I want to be able to make sure I can contact my, my colleagues, my work -- my workers, my bank, and it's just a question of how we do it. I think that's the most critical part. I think we're a long way there by having these discussions. The things I'm most interested in, right, is making sure that when we have this discussion that there is proper oversight and accountability of how we share this information across the different parts of the private sector and the government. Making sure that there is proper public oversight, if it's very personal to us then we want that part of our government with the greatest accountability to have responsibility for. That's why I think Gen. Alexander's suggestion of Department Of Homeland Security being in the -- in the saddle at the center of making that happen I think is critical. Making sure that we're very smart about what information is shared, at what level of detail, and the question of how -- how personally identifiable information that perhaps won't be necessary, like the easy pass analogy. I -- I'm stealing your script, but I'm sure you will sing it much better than I.

Keith Alexander:
Explain it for people. Go right ahead.

Anthony Romero:

The idea of just being able to have certain data that's collected that sends off certain bells and whistles within the sector that says, "Okay, this might be of concern," but not collecting everyone's information in a massive aggregation that gets sucked into a major central database. I mean, there are ways for us to really throw the switch that's very specific in terms of what are we looking for from where, what type of information, what type of -- and that's good national security. As we always said before, the problem with good intelligence is to finding the needle in the haystack, and you make it all the harder when you throw more hay on the haystack to find that one needle. So we do ourselves a service in keeping better national security by being smart from the beginning about that which we're trying to identify and for what purpose.

Steve Inskeep:
Go ahead.

Keith Alexander:
Could I add in? I agree with everything that you said. In fact, I'd like to just put on the table the team, the cyber team that our government needs here. I -- as you correctly stated, I see DHS as the entry point for working with industry, and I think there are great reasons for that. The transparency, everybody knows we're doing this exactly right, and when you look at this, this gets the best of our team together. So you've got DHS doing that. There's a lot that we can do to help them on the technical front, FBI, NSA, and Cyber Command, and we should work together as a team to do that. FBI would have the lead for the law enforcement and the attribution parts of this, and NSA on the foreign intelligence, and Cyber Command on defending the nation. And together that team is what I think the American people hold us accountable for doing.

And you'd expect, as we discussed earlier, that's where you want this team to get together, and make sure it works right. Have it transparent with oversight, but everyone here knows -- and the analogy of the car I think is a -- is a good analogy because what we're asking industry to do is to look -- if you see these kind of bad things going on, let us know right away. Let the government know. It's just like calling for fire alarm, 911. Call us, and we'll respond. And if -- otherwise we don't need to know what traffic is transiting.

Steve Inskeep:
Congresswoman.

Jane Harman::
Could I just raise something Steve at this point? I -- how many people here have been hacked?

Steve Inskeep:
Number of hands going up, okay.

Jane Harman:
That's pretty -- and how many aren't sure, but think maybe, sort of, kind of you were hacked?

[laughter]

Steve Inskeep:
How many don't want to admit it?

[laughter]

Jane Harman:
And how many don't want to admit it? But it's a big portion. I think it would be helpful is why I'm just -- while we're defining the problem to, to be a little more specific to people who are here for a reason. They want to understand the subject, and I hope participate in the best solution. How does this work? I mean you're training DHS to look for what? And the public should understand, they're looking for what? And let's -- here's our civil liberties bells and whistles person over here. His level of comfort matters, because obviously the goal here is to do two things at the same time. One is protect our country and our infrastructure, and the second is protect what -- why we are a great country --

Anthony Romero:
Right.

Jane Harman:
And that's our civil liberties and our Constitution. So could somebody maybe be a little more specific about, what -- how do you -- how do you know the red car is going by?

Keith Alexander:
So, there's a couple ways, but first I do have -- I got from Norton Study 2012, 72 percent of people online have

been hacked or victims of a cybercrime. So that means your chances, it would be three fourths of the room, and the other quarter they have no yet gotten to. So it's significant. How that works, and how the antivirus community does it is by -- we call it signatures, but it's actually signatures and different techniques that you see, and things like that. What's a signature? It is something that they have -- think of this as a scan. When you go to the grocery store you scan in your food for money, and you have this barcode that goes by. So think of it as a barcode, and it lets all the barcodes go by except for this one version, or these several versions. Maybe all these that have this version is alarmed by the Internet service provider, as an example. And they say, "I've got a problem here," and it can be done without a human in it. It actually is done by a machine that says, "I saw the red car," or a bad think happening. I tell the government we've got a problem, and that red car was coming from point A going to point B. So we know it came from there, and we know it's going to there. So this company is the potential target. So you know all that, because of the way the packets and stuff in the network go. So --

Steve Inskeep:
You're saying the key is to identify, to be able to recognize a particular virus, a particular worm as it moves around.

Keith Alexander:
And potential --

Steve Inskeep:
And spread the word of that.

Keith Alexander:
And, and it gets a little bit more complicated, but that's in essence the way it all works. And it's done by the -- actually the way the packet is and what's in the packet, the Internet service providers do that as a service today. They do that so that your networks operate securely. They try to weed out as much as they can, and what they'll tell you is they have a limit to what they can do because of where they are technically. So we know some information. Other parts of industry knows information. FBI and DHS has information. If you want to really make it secure what we would say is -- you know the American people would say, "Well, why don't you work together?" And that's the whole

intent. We've got to work together so that each of those missions can be done. I think, you know, when I was mentioning back, I think our Internet service providers are extraordinary. They do a great job, but they would tell you it would be better if they could partner. Now there's some -- there's some issues that have to be put on the table. The transparency is one, liability is another.

Steve Inskeep:
Well, let me let Anthony finish the point there if we can, because when you talk about transparency, I mean you're saying that it is essential for the United States government to be involved with companies that virtually all of us use, with which we entrust our most sensitive information in many cases. And for the government to have a dialog and discussion with them that might involve a lot of -- being very close to a lot of intimate information about our lives.

Anthony Romero:
But I think that's where it's all a matter of who is tasked with the job and that if you have a Department Of Homeland Security which is raison d'etre. And we've often heard criticisms, sometimes publically that the Department Of Homeland Security is not up to the job. Well, that is their job. It's almost like saying it is your job to defend the homeland, and if they can't pull this together then we have to have a very different conversation about why we have a Department Of Homeland Security that can't defend the homeland from one of the most critical, far ranging areas of threat. And so many of the criticisms we've heard from individuals in the Senate and the House, luckily we've had the leadership of Senator Collins, have said, "Well, DHS can't do it." Well, they must do it. That's the reason why we're there. If not we have to have a very different type of conversation about DHS.

Steve Inskeep:
Okay, what is DHS's involvement in cyber security right now? Just lay out that ground work, the basics.

Anthony Romero:
Frankly, it's often unclear to us to the extent in which there is information sharing, and there is an involvement. It's at a very low level. It's not very forthcoming. They certainly, in my opinion, general, you know this much better than I do, but it's -- they're reluctant

participants on these discussions. They feel like they have a lot on their plate. I think that you have had very, kind of key individuals here on this table making this point much more salient. Joseph Nye at Harvard has been brilliant at raising this concern more publically, and so I think it's gotten the attention it deserves. But for me the reason why DHS must be charged with it is because there you ensure the accountability. You have an ability in terms of getting information to the various members of Congress. You have an office of Inspector General. You can have a GAO report. You can have hearings called by Congresswoman Harman to make sure that we have these. You --

Jane Harman:
Senator Collins.

Anthony Romero:
We're not -- we're not capable of having that level of civilian oversight if it were placed, with all due respect, general, in the Pentagon. It just -- it's a very different beast, and so when you're talking about something as significant as a personal, identifiable information of Americans and how we interact with the world, I worry if that is in the domain of a military complex where it's harder to shine the light in those black boxes.

Steve Inskeep:
First, Congresswoman Harman, they would probably let you still call a hearing if you wanted to.

[laughter]

Just a second if I can, because you were directly addressing the -- do you -- do you agree with what he just said regarding the fact that -- regarding the idea that a civilian agency needs to be the lead on this as opposed to the military? That was the statement that was made.

Keith Alexander:
I think given where the discussion is I believe that's the correct thing to do, especially if we can handle the technical problems of allowing FBI, NSA, and Cyber Command to do their jobs. Then yes, it allows for the transparency which I think the American people need in this area. Cyber is so important to all of us. You want to know we're doing it right, and the way to do that is to be transparent, to

put that out. From my perspective, we can do both, and we should do both. And I don't have a problem with that accountability at all, and that transparency. And as I mentioned earlier, this is a team. We all have to work together. And I think by you knowing that we're working together, not one of us individually, you know that we're going to do this right.

There's some other things though, and I think Senator Collins is going to bring this up. So I'm going to pass this to Senator Collins, because --

Steven Inskeep:
Go right ahead.

Keith Alexander:
My experience with DHS is they are growing, and they're coming on fast. Secretary Napolitano, Mark Weatherford, and their cyber group are doing a good job. They need help. We are helping. We've got to work together as a team, and from where I sit it's our job to help them be successful. And they will get there. They are, they are taking the right steps, and I think that's the right thing to do. Now we can -- we can throw rocks at them, but the reality is I think our nation needs them to be in the middle of this. And so I'll pass it over to you.

Susan Collins:
I just want to clarify what DHS's role is now. First, it's responsible for the dot-go domain. In other words, the civilian agency's computer security. Second, it's responsible for being the liaison to the private sector. And third, it's responsible for critical infrastructure. That's not a new responsibility. The department was given the responsibility for securing critical infrastructure in the Homeland Security Act of 2002. And so I think it's important to understand what the domain -- what the responsibility of DHS is now. It does not have responsibility for the .mil part of our government. It is not -- it does not have the expertise of Cyber Command or NSA, but it does operate a 24-hour watch center --

Keith Alexander:
Right.

Susan Collins:

That is called the National Cyber Security and Communications Integration Center. I just call it the Cyber Security Center, but the insiders call is NCIC. Don't ask me why. It is responsible for monitoring in real time what is happening in the dot-gov space, and it probably will not come as a surprise to you to note that the cyber preparedness of our civilian agencies in the federal government has a lot to be desired, and it various enormously from agency to agency.

Now, at this center are representatives of the private sector, from NSA, from the Department Of Justice, from the Department of Commerce, and they're all working together as a team approach. And that's what it takes, and that's what the bill that Joe Lieberman and I wrote. What it codified is a team approach to establishing cyber standards, best practices for the private sector to voluntarily adopt, and in exchange get liability protection. But DHS cannot do it without the help of NSA. That's absolutely critical, because NSA is always going to be the expert, but NSA does not have the relationships with the civilian agencies and with the private sector and with the critical infrastructure operators that DHS does. And that's why that partnership is essential.

Steve Inskeep:
Is there now, does you bill create, or does there need to be a central person who is accountable and responsible? A director of national intelligence, so to speak, for cyber security?

Susan Collins:
That's an issue that we've struggled with. At one point the administration wanted a cyber-center within the White House, and there were a lot of us with qualms about that for actually reasons that I think Anthony will be very sympathetic to, because that person is not accountable. Any time you create a czar-like position within the White House we can't call the before Congress to testify, to be accountable, to be questioned, and so that is not the approach that I think is best. What we finally have come up with is a council that would be chaired by the Department Of Homeland Security in our bill, but would have a broad range of representation across the federal government.

Steve Inskeep:

I wonder if -- and we're going to get to you Anthony in a second, but I wonder if, in the end, cyber threats are a little like the word, "terrorism." It can be a catch all word. It can catch a lot of, lot of different threats. It's actually a technique of attack that many different agencies you would want to share information, but it's not a fundamental problem that needs to be attacked as a problem. Is this what you're suggesting? I mean it's just so broad.

Susan Collins:
It is broad, but it's a fundamental problem nonetheless, because our society is increasingly a wired society. And if you'd think back we've had building codes forever, for generations to make sure that if a building is constructed that it meets certain standards for the electrical wiring and for the plumbing. Well, now that we're in a society, in an economy in which computers operate virtually everything, and industrial controls are so critical to the operation of everything that controls the basic necessities of our life, it seems to me that we've got to have standards that are met, and the best way to do that is through a collaborative system that draws upon the expertise of the private sector and the knowledge of government.

Jane Harman:
Maybe there's one other metaphor or example that would fit with what Senator Collins was just saying. I'm from California, earthquake country, and buildings, and freeways, and whatever have to meet certain seismic standards. Otherwise it all falls down and hurts all of us. I would think that this is similar, and think floods and tornadoes and so forth in other parts of the country. Minimum standards have to be met or the infrastructure falls down. And this critical infrastructure, the whole cyber world makes everything else, basically everything else work, and so I guess your argument is there are minimum standards at least on a voluntary basis -- I think you changed it from mandatory to voluntary -- that have to be met, or this whole network that supports all of us falls down. Correct?

Steve Inskeep:
Anthony Romero.

Anthony Romero:

But I think -- I think your analogy is exactly the right one. The cyber security issues certainly evokes the debate around terrorism, and of course they're related. They interacted very directly in the aftermath 9/11, and I think part of our concerns in getting the details right, and asking the pesky questions. We were teasing each other before about making sure that we were working nicely here on the podium in front of everyone, but --

Jane Harman:
[laughs]

Anthony Romero:
And that is of course our way, because we're civil libertarians after all.

[laughter]

But it's also because of a history.

Jane Harman:
[affirmative]

Anthony Romero:
And in the name of terrorism, fighting terrorism we tortured, we abrogated due process for certain detainees, we opened a military camp in Guantanamo that remains open to this day even though this president and many wish to close it including Senator McCain from the Republican party. And so we did many egregious things that we have now come to regret. In the name of national security and cyber security we could easily go too far as well, and we don't have to go that far to remember this. I've only been the director of the ACLU for the past 12 years. I lived total information awareness, operation TIPS, Terrorism Information Protection System; the NSA leak that was leaked out to the New York Times; the questions around the Patriot Act provisions, about getting library records without proper oversight of Congress. And so when there is a bit of energy that is of -- around what are sometimes difficult policy issues I think that's to the good. I think we've done our job. I think that's what -- that's what democracy looks like, and the reason why people are worked up, or concerned, and sometimes sending pesky letters or pesky floor amendments is because we got it wrong for a number of years. And when you're talking about the very personal

information of people in their everyday lives we want to do our best to get it right.

Steve Inskeep:
Help me define the problem there. What is an example of something the government could plausibly do in the name of security in this area that would scare you?

Anthony Romero:
Well, I think -- I think certainly locating any of this information, gathering, the cyber security concern within the military or the NSA, I'm not buying it. You've given too much power to it, too obtuse, can't get it, we litigate over to the military every time. We litigate the CIA. We litigate the OD. Give me the civilian agencies any day. If you're going to adhere to the rule of law give me an equal playing field.

Steve Inskeep:
Even though they're the guys who may have the expertise, and may be able to get the job done?

Anthony Romero:
We are the American government. We are the United States of America. If you're telling me that the military is the only thing that can work then we're in a very different country than one I want to live in. No offense, general. I want my civilian part of my government to work just as well as my military. So if you tell me that the only thing that works in America is the Pentagon then I want to renegotiate my taxes with this government.

[laughter]

Jane Harman:
We have civilian oversight of the military in this country, but, but the Gen. Alexander just said, this is why I'm up here sitting right next to you my friend [laughs] with great love and affection, he just said that he welcomes --

Anthony Romero:
Yes.

Jane Harman:
-- civilian oversight of this problem by DHS, and he and a group of folks on his committee or at least informally until we have this much needed legislation -- I'm very

objective about this -- are helping DHS get up to speed. So that concept is fine.

Anthony Romero:
It's retired. Then I think the level of personal identifiable information, just making sure you don't collect everything on everyone that just gets sucked into some, kind of central system that people can get access to. Because let's face it, that is often happening in other contexts. Facebook, the idea that everything I've ever posted -- and I don't have a Facebook page, because I refuse. I'm the last one who gets invited every day to join Facebook -- but the idea that your personal information is theirs forever, and everything you put is theirs for them to own or for them to market is just a frightening thought.

Jane Harman:
That's a private --

Anthony Romero:
That's a private sector.

Jane Harman:
-- concern.

Anthony Romero:
I know, and we don't have the control to manage that. If I could -- if I could find some exercise over the Facebook policies I'd love it, but the American government is different. Why? Because only the American government has the ability to take away your freedoms. Facebook can't come and arrest me. They can't seize my bank accounts. They don't have the powers of the police state. The government can take away my liberty the most fundamental way. They seize my assets. They can restrict my movement. Facebook can make my life difficult if I choose to be on Facebook. The American government can lock me up, take my assets, could put me on a watch list, could inhere my ability to travel on airplanes throughout the public -- throughout public spaces. That's why it's so much more critical to get this right when we're talking about the government owning and possessing this data.

Steve Inskeep:
Let me make sure that we define that as well, Gen. Alexander, just so that people understand, what authority

if any do you, or does your agency now have to look at the information of U.S. persons, of American citizens and others living here of their bank accounts, of data centers, whatever the reason might be? What authority do you have? What authority would you envision having?

Keith Alexander:
None right now without a warrant, and it would be normally through the FBI or something like that.

Steve Inskeep:
Correct.

Keith Alexander:
Now let me, let me go back, because I do -- I do want to just push back a little bit on Anthony here.

Steve Inskeep:
Sure

Keith Alexander:
Because I haven't been in the agency as long as you've been at ACLU, but I've been there over seven years, and they said I have to stay until I get it right. So it's going to take a while. I'm an army guy.

Steve Inskeep:
[laughs]

Keith Alexander:
I am absolutely impressed with the way our people deal with Americans' civil liberties and privacy, the way we ensure that our civil liberties are protected. Everyone at NSA has to go through a course because in the collection of our stuff overseas we're going to see American data. And we protect that, and we respond to the House Permanent Select Committee on Intelligence, the Senate Select Committee on Intelligence, the Department of Justice, the Pentagon, the DNI, anybody else. And every time we make a mistake we self-report, and we correct it. I don't know of anybody else in government that goes to that extent to ensure that we do this right.

Anthony Romero:
That's only because, with all due respect, sir, with great fondness and affection --

[laughter]

Keith Alexander:
How great.

Anthony Romero:
Only because the NSA got caught with its hand in the cookie jar twice now. Once with the whole effort with Roger Bamford and others who was clearly involved in surveillance and shouldn't have been. Secondly in my mind, although Congress gave President Bush the get out of jail free card by authorizing NSA through the FISA Amendment Act -- the FISA Amendments Act, which gave them the power after the fact. And the only reason why I'm concerned is because it is -- I'm sure it's true. I know that the men and women in uniform who occupy your role, many of them I've met over the years. I think many of the women in the intelligence community are terrific. Bob Muller is a terrific man who cares about these issues, great integrity. I've sued him a half a dozen times --

[laugher]

-- in the last six months.

Jane Harman:
That's how he shows the love.

Anthony Romero:
But, but I --

Keith Alexander:
Is this where the Taser comes out?

Anthony Romero:
I agree to disagree with him. But the concern I have about the military is that it really is quite a different thing when we're thinking about -- and I think this where you and I completely coincide philosophically -- with Americans' data it should not be -- the locus of activity should not be our military. It should not be. I mean it's what we expect of the civilian agencies of our government. And I think at the end of the day, I think that the biggest concern is that is so much that's there. And it's not like I've done anything wrong. My -- we do -- we talk about this all the time. Well, what do I care if the government should access my email inappropriately? You know, I've

done nothing wrong. I'm not breaking the law. I don't want them to see some of the interaction between me and my nephew, you know, the embarrassing things. He's a teenager. I'm trying to explain to him certain aspects of adult life which I don't really want to embarrass the poor fella about asking me some of those key questions in a email. How am I going to write the answer back in proper language that he can understand that won't get caught by the filter that he might have on his computer? You have to think about these things. I want to teach a young man how to be a responsible adult with his body, with other people's bodies. You want to have those discussions properly, and you don't want the government picking up that conversation between and uncle and his teenage nephew. And that would be mortifying for a teenage nephew to have his communications picked up and asking uncle a question that he thinks that he knows already. Just little things in every day aspects of one's life you just don't want the government to pick up. And I think finding the proper restrictions around it, finding the proper locus of activities, finding proper oversight with our members of the Senate and the House, I think are a key part of it and making sure we get it right because we've gotten it wrong.

Steve Inskeep:
Senator Collins is about to offer some oversight. Please, go right ahead.

[laughter]

Susan Collins:
First, I want to speak to this because I don't want there to be an impression created that the bill that we tried to get through would in any way allow the situation in that Anthony just described. And I think there's a lot of misunderstanding in this area. First of all, and the general can speak to this better than I, but he educated me on this issue. The so called digital signatures that we're talking about here are ones and zeros in various patterns. They aren't the content of emails.

Anthony Romero:
Right

Susan Collins:
They are being used to identify dangerous malware or attacks that are coming into the system. Second, our bills

specifically make sure that any information that the private sector gives to the government related to cyber security is -- there's a horrible word for it, but it's something like anonymized [spelled phonetically].

Anthony Romero:
Right

Susan Collins:
And that word obviously speaks to the fact that any personal data related to it that would be -- help you to personally identify an individual would not be transmitted. And so there are all these safeguards --

Steve Inskeep:
So, is this the equivalent of wiretap phone calls? They're supposed to stop listening if there's personal discussions going on in a wiretap phone call? That's what you're -- it's the digital equivalent to that? Is that what you're saying?

Keith Alexander:
No. No.

Steve Inskeep:
Help me out.

Susan Collins:
No. It doesn't work like that and I will let the general -- since he can describe it.

Keith Alexander:
So, what you're actually -- what you're actually -- it is kind of interesting we're arguing over a bad guy putting something in your email, sending it to somebody else, to do something to him that you didn't know was going on. So, ironically, both of you want to know that that's occurring. And what happens is, the machines can see signatures. They can see those go by, and alert on them. There is nothing about the traffic or the communications that the government will get, civilian or military. So, nothing in the communications come to the government. Only the fact, let's call the signatures A through a billion. We have a billion signatures. I think MacAfee is up to --

Jane Harman:
By nothing you mean; no content.

Keith Alexander:
No content.

Jane Harman:
Right.

Keith Alexander:
That's right. So, all you're going to get -- let's call the signatures and numerate them. Start with A. So, signature A goes by. All the government needs to know: DHS, FBI, NSA and Cyber Command is that A event occurred. We don't need to know anything more about the communications than A occurred. And so, what the government finds out is A occurred and it was going from point A to -- from one point to another. Can't use point A because it was in the A. I get it. I think you do. So, tracking that, what that means is all the government's being told is this. Now here's a great point about where we are in the Internet today: Everything we do in this area is auditable, 100 percent. As it is with what NSA does in our activities; a hundred percent auditable by all the agencies I talked about. So we have everything that we do is 100 percent auditable. In this area would be, too. And the key, the reason that I really believe that DHS is in there so you all know we're doing this right. It's transparent. It is being done right. We've got everybody working together. It is a great way and actually, you know, you want us to defend the country against an attack. You don't want us to be in the middle over here operating in the country trying to set something up or working with industry when we should be defending the nation. So our job is to defend the nation.

Susan Collins:
If I could just say one quick point. Our bill has vigorous oversight in it. It requires regular reports by all the IGs, by the GAO, and by the Privacy and Civil Liberties Board, which by the way, this administration was extraordinarily slow to appoint, members to, which has always been baffling to me.

Steve Inskeep:
I just want to make sure I understand the basics, then I'm going to open it up for questions here Senator about your bill. You've just described the search for digital signatures. If I'm not mistaken, you're describing

something that goes on all the time now. That the government tries to do on its own systems. Go on. Yes?

Susan Collins:
There isn't information sharing to the degree we would like to have.

Steve Inskeep:
Right. That was the next -- you're talking about something that, individual organizations, in theory, at least, try to do to protect themselves. My own antivirus protection on my computer may try to do that. Your bill is an effort to increase the cooperation between different institutions and corporations as they share information so that they can all be looking for threats together. Is that correct?

Susan Collins:
Correct. And if there is a major breach in critical infrastructure it has to be reported. What happens now is a lot of companies try to keep this quiet.

Steve Inskeep:
Sure.

Susan Collins:
They're worried about what the reaction of their customers and clients would be. So, they don't want a report. We want to give them incentives to report. We want to require them to report if it's a major breach, but we want to give them incentives by giving them some liability protection.

Anthony Romero:
Here is what I want to be clear. That the bill that Senator Collins is describing, her own bill, with Senator Feinstein, and Lieberman, is I think it strikes the right balance. I mean there are very many parts of it that we think are absolutely right on the money. There are always things that we disagree on. I mean, we can't help ourselves, senator. So you'll just have to forgive me for the "sins of the father visit on the children," but in by and large, that's the right framework.

Now, there are other models being thrown out there that I think are highly much more problematic. Which are much more reminiscent of opaque data collection in different parts of the federal government that have us much more worried. And I think the most important part is this

debate. I mean I really do keep coming back to it; the idea that we're having this discussion prior to rather than after the fact is critical. And let's work on figuring out the details.

Steve Inskeep:
One quick question on the bill before we go to questions here, senator. You mention that these are voluntary, voluntary rules. People would sign up. They would get incentives of various kinds. Ms. Harman used the analogy of building codes, though. Building codes don't tend to be voluntary.

Susan Collins:
Sure.

Steve Inskeep:
Why make these requirements voluntary? Why not mandatory?

Susan Collins:
Our bill originally make them mandatory and gave the liability relief. Frankly, it was a calculation on our part, that the private sector would be less worried about the bill if they were voluntary standards and that the incentives were sufficient that they would participate any way, particularly when we made it very clear that the private sector would be involved in developing the standards. So it was partially a policy calculation and a political calculation. In the end, I don't think our change from mandatory to voluntary standards brought us a single extra vote in the senate, but that was the decision that we made.

Steve Inskeep:
It's so rare that things get bottled up in Congress these days.

[laughter]

Steve Inskeep:
Surprising that would happen.

Anthony Romero:
Sometimes a bottle up is okay. When things get trammeled through like the Patriot Act, without a bottle up, with too little debate, and lack of knowledge, and lack of transparency, that doesn't make democracy look any better.

I mean, the reason why we have two branches of government and the Congress -- three branches of government --

Steve Inskeep:
Three branches of government.

Susan Collins:
Three branches of government:

[laughter]

Anthony Romero:
I misspoke. Three branches, two houses, right?

[laughter]

-- is because we believe in a series of checks and balances. Checks and balances make democracy messy, contentious, sometimes slow, sometimes an impasse. That's what democracy looks like.

Jane Harman:
Could I just say one more thing, Steve?

Steve Inskeep:
Go right ahead.

Jane Harman:
Since I've behaved myself pretty well. As someone who was in our Congress during those years, and tried very hard to get full information, it was frustrating for members of congress, too. And many members of Congress felt there needed to be, and there still needs to be, a robust debate in the public square about a basically -- my version a new legal framework that fists the requirements of a 9/11 world, which is a different world. But the public has to be part of it. I think Senator Collins is right about the Privacy and Civil Liberties Board, which was required in the 2004 Information Reform Law that was worked on together and has never been vigorous. Not yet. Not under Bush or the Obama administration. And the goal is, and I think Gen. Alexander would buy this -- I just thought I'd include it on a note of unanimity here for the -- I could never remember this word, but the mutually reinforcing values of security and liberty to be factored in at the same time when we make policy. It's not a zero sum game. You don't get more of one and less of the other. You either get more

of both, or less of both. And so the conversation here today, is about how we can do both. And how we can do it in a way that the public understands, or how our government can. That the public understands.

Anthony Romero:
There's one reason why I think we need to figure it out, also at the beginning is that very often, the public and the effected communities are not in a position to question after the fact. I'll give you one example: The FISA Amendments Act allows the U.S. government to intercept my U.S. citizen emails when I'm overseas or if I'm emailing them overseas. So, if my sister's in London or my nephew's in London, let's say. The same little nephew that I'm trying to explain the bees -- the birds and the bees to happens to be in Mexico, and he's asking me a question, my communication to him can be intercepted to Mexico without court oversight. Whereas, if I'm emailing him from Florida, it's protected. Now, wherein the Supreme Court, the ACLU is arguing this case in the Supreme Court, October 29, where the issue is, do we have standing to question this law? We have humanitarian groups. We have human rights groups. We have groups in Egypt who are collecting data on the activities of their countries. They're emailing them to us so we can interact together as human rights campaigners. We have Guantanamo lawyers who are representing individuals like Guantanamo Military Commission, who will try to interact with family members overseas in some of the hot spots. Attorney/client privilege is implicated. But you have no proof that those emails are being intercepted. So the individual, we are now asserting, we can show the harm, because the harm is chilling our ability to do our work. And so that's why you have to get it right from the beginning, because you can't challenge it after the fact.

Steve Inskeep:
That's the third branch of government, right? Just to be clear on that.

Anthony Romero:
It's the Judiciary. Three branches.

[talking simultaneously]

Keith Alexander:
I was going to say, it just came up, the third branch.

Steve Inskeep:
Okay, good, good. All right, let me invite your questions. I'd like to state a couple of rules. I believe there's a microphone or two that will come to you. If you have a question I would ask you first to state your name so we can get to know each other at least a little bit. And make it a single direct question so that we can get as many of you in as we can. We'll go right to the back. Please go right ahead back there, ma'am. Go ahead and stand up so we can see you.

Jen Scholtes:
Jen Scholtes from Congressional Quarterly. And this question is for Senator Collins. I was just -- you said that the change in the bill to make things voluntary didn't get you -- probably didn't get you any votes. I know that if you knew it would get you the votes, you would've done it but, either this Congress or in the next, or the one after that, where do you see any of these tweaks coming that you think maybe that can move this?

Susan Collins:
Well, I certainly hope that this isn't a case where we have to wait for a cyber 9/11 before action is taken. It is encouraging to me that although my close partner, Joe Lieberman, will regrettably be retiring, that the next person who will be the chairman of the committee or the ranking member is also a cosponsor and involved in the bill, and that is Tom Carper. This problem is not going to go away regardless of who's in charge in the administration, regardless of who wins the presidential election. The problem is only going to get worse. The number of attacks has grown exponentially over the past couple of years and it's going to only get worse. I'm reminded of the words that Michael Chertoff and General Hayden said when they essentially said they were haunted by the fact that there was intelligence prior to the attacks on our country on 9/11 but that no one connected the dots. And if they had done so perhaps the attack could've been averted. In this case, the dots are already connected. The alarm has already been sounded. And we know that it's only a matter of when, not whether we have a catastrophic attack.

So my hope is that this isn't a case where Congress does nothing until there is a catastrophic attack on our

critical infrastructure, and then inevitably we will overreact and pass legislation that will make Anthony very uncomfortable, and many of the rest of us as well. So, my hope is that after the election cooler heads will prevail and as more and more people get educated on this issue, and determined to do something about it, as more and more companies have the personal experience with a cyber-attack, that we can build enough public support to get the job done.

Steve Inskeep:
So you see it less a matter of -- more a matter of public awareness and politics than changing bill in some way that you can find?

Susan Collins:
I do.

Steve Inskeep:
All right, couple more questions. There's time. Back there Sir, go right ahead. In the back row again, then we'll go to you in front of him. Please, go right ahead, in front of the cameras. Yup.

Zach Biggs:
Zach Biggs, Defense News. I'm curious General, you said that a couple of concerns the Senator mentioned being, protecting critical infrastructure and protecting intellectual property, were, I believe you said, "solvable." I'm curious, what does that mean as far as what would it take to solve those particular issues?

Steve Inskeep:
Hand the microphone to the gentleman in the front of you.

Keith Alexander:
Thanks, because I want to clarify. We're never going to get rid of 100 percent; so when I say solvable, what I mean is we can mitigate most of the problems that we're seeing on the network today. When you see how the defense networks, with one level of protection is able to operate, the rest of government at a different level, the first thing you say is, "we ought to fix that, and we ought to work this together." I'm happy to say that DHS and the defense department are working together to address that problem. Then the question that you pose is; what about critical infrastructure? You know, the defense department

and DHS isn't here to defend the government. Who's defending the nation? And the answer is, well, that's probably the government's responsibility and here's how we have to do, we have to partner together. And so from my perspective by putting all the information on the table so the Internet service providers and others have access to that information, within industry and from government, that's what it takes to help mitigate this. And I think we can mitigate a large portion of it. What that does is takes much of the junk out of the system and allows us to look at the more persistent threats. And that's what we need to get to.

Steve Inskeep:
Gentleman that now has the microphone, go right ahead. Stand up.

John Reed:
John Reed with Foreign Policy. So, there's already a program in place where the Defense Department and the intelligence community and defense contractors can share information about the cyber threats and it's being expanded to include DHS possibly, and critical infrastructure providers. How does that relate to the executive order that's working its way through the White House and also the need for legislation? I mean, how do they relate? Is there still a need or what is the need?

Keith Alexander:
So, I believe there is a need and I can address the Defense Industrial Base Pilot is a way of working -- exchanging information not in real time and without the liability protection, and it's between the Defense Industrial Base, those companies that work with the Defense Department to help them protect their information. We exchange information out of the at an unclassified and a low level classification level. It doesn't give us the ability to work with the Internet service providers and allow that to benefit the rest of the critical infrastructure and the rest of government. So, that's really what we need the legislation for, is to work industry and government in this way.

I think, as we've done in the managed security services, we've now given that over to DHS to run for the government, and we provide the technical assistance. I think that's a

big step forward and it shows you a step towards what could be done in legislation for information sharing.

Steve Inskeep:
You said several times, “liability protection.” I just want to make sure I understand what that means on a basic level. You’re saying that a company is telling the government, if I’m going to let you into my systems, if I’m going to share information with you, I need to know that I’m not going to be sued for some problem that arises from that. That’s on a most basic level. And do you want to answer this question about how far the bill goes beyond what’s already been done, senator?

Susan Collins:
Yes. First of all, I totally agree with the general’s analysis of the -- what’s known as the DIB Project and having it expanded, but there’s no way it’ll have the breadth that would be brought about our legislation.

I want to also touch on the executive order that you mentioned. I personally believe, that while I understand and share the president’s frustration over the failure of Congress to act, that the executive order’s a big mistake. First of all, the executive order cannot grant the liability protections that are needed in order to encourage more participation by the private sector. So, the executive order simply cannot accomplish what legislation can. In addition, an executive order is not lasting. We need -- and it doesn’t reflect a consensus by Congress on what should be done. So, I think the executive order is a mistake. I’ve urged the president not to pursue it, but rather to continue to work with us. And I fear that it actually could lull people into a false sense of security that we’ve taken care of cyber security, and the executive order simply cannot do that.

Anthony Romero:
The one thing that I might add to Senator Collins is that, in addition to the fact that this needs a thorough debate and both houses of congress engaged with a piece of legislation that could outlast a president. Any action by any occupant of the White House on an executive order that either mandates a collection of data across federal agencies worries me. And just because President Obama, who might be a bit frustrated at the gridlock in Washington, that’s what we’ve got. And it’s not going to be President

Obama forever. And we've had President Bush and we used to -- using those executive powers for good reasons and we'll find them used -- turned right on us in -- for bad reasons in subsequent administrations. So I completely agree with Senator Collins that that cannot be the full-time or the long-term solution to this issue. It's misguided, it might come back to -- backfire on us, and it's just not going to solve the problem on a long-term issue like the one that she's outlined.

Steve Inskeep:
Got time for a few more questions. Does anybody closer to the front have a question here at all? Oh, okay, I guess not. But there's one in the back. Go ahead ma'am.

Lillie Coney:
Thank you. My name is Lillie Coney I'm with the Electronic Privacy Information Center. I want to ask a question about oversight, congressional oversight specifically, you've spoke a lot -- a great deal about internal agency oversight IG, all of it very excellent. But the complexity of cyber security for government agencies and non-government entities, I was wondering if you we thinking in terms of what needs to happen so that congressional oversight is up to the task of protecting privacy and civil liberties? But specifically looking at the structure, staff, skill-sets, organization of committees thinking more creatively about keeping up with oversight responsibilities of congressional committees. Thank you.

Susan Collins:
In our bill, all of those reports that we would mandate in our bill from the IGs of various departments -- inspector generals -- from the Government Accountability Office and from the privacy board would be reports to congress. And if I'm the chairman I can assure you we would have hearings on those reports, but the -- those reports are, in many ways, an action forcing mechanism. By having those reports out there out there, available to review by your organization, by the ACLU, by other privacy groups, it will prompt congress to take a close look at them. IG reports, we pay attention to. When an inspector general reports an analysis, and Jane Harman and I, when we helped to write -- we're one of the four authors -- we're two of the four authors of the Intelligence Reform Act. In 2004, we insisted on having that privacy board, which is we've been so disappointed that two administrations now have really

sort of brushed it aside. And it's something we're going to continue to push on.

Lillie Coney:
What I'm specifically asking about is this is a highly complex area --

Susan Collins:
Right.

Lillie Coney:
-- where cryptographers, you need security expertise. If you're looking at bulking up the technical expertise within the committees themselves to be able to engage in peer to peer discussions with agencies, with industries as they look at the information coming in to better inform and bulk up the resources of the committee to engage at a higher level.

Susan Collins:
Well, even being in the minority, I have always had an attorney on my staff who is assigned privacy issues, and I've always placed a great premium on that. I'm not saying that the expertise is equal to that that we might find in some advocacy groups, but we interact with those advocacy groups and that expertise does exist in the oversight offices that would be reporting to us. So I really don't see that as being a big problem.

Steve Inskeep:
Let me ask you both, because we have two people who've been on sensitive committees, are you confident that you have the time as busy lawmakers, the staffing as senators and members of Congress, the access to really get into what a variety of agencies, including intelligence agencies are doing on any given sensitive topic?

Susan Collins:
Do you want to do intel?

Jane Harman:
I think I hinted before that I asked for a lot of material that I never got. And I think Congress over a long period of time was shortchanged. I think that is improving. And as I mentioned I serve on the advisory board to Jim Clapper, the director of national intelligence, who has reviewed with me and others on that board what he does to

keep Congress fully informed. I think members of Congress have an obligation to do deep dives in areas that are of critical importance. That doesn't mean that every member has to know about this issue. I can tell you this member of Congress over here would astound you if you had enough time to learn what she knows, and I've seen her briefing books at night. I mean, she is no fun, just no fun. All she does is work. But seriously, some members of Congress take this responsibility very seriously some staffs in Congress -- and I think you would probably know that I'm a former staffer, so is Susan Collins -- take this very seriously. And Congress has the capability. I think the frustration with Congress right now is that the place is broken, not the people. There are many talented people in both parties, staff and members, who would like to contribute more, but the paradigm now is one party blames the other party for not solving the party and then they never work together, which again is underlying this: Working together to solve a problem is the way to get the best solution. Which is why it is very heartening that the person to my left sitting up here has said in every way that I've tried to hear, that he's going to be part of the solution of this problem.

Anthony Romero:
I'm part of the solution, and I will be part of the next solution.

Steve Inskeep:
Let me ask you about congress. Are you confident that congress has the capacity to provide oversight in this area?

Anthony Romero:
No. And that's okay because with oversight from Congress -- I think Senator Collins said it -- with the reports that Congress -- then the public does. It's these opaque oversight mechanisms which worry me the most. We all pay attention to the OIG reports, they've been incredibly -- the Inspector General Reports have been incredibly important. GAO reports, if you can get them in time and they can focus on the right issues, they can be incredibly important. More importantly are the reports that are mandated from the government agencies themselves to congress. It's only the reports on the Patriot Act -- the use of the Patriot Act provision that we got to see how many tens of thousands of requests using these library

record provisions -- section 215,219,217 -- that's the only way we knew it. Warrantless -- warrants, you know, that -- where they're able to get information from individuals without court oversight. That's the only way we got it. That's the only reason why we have a fighting chance on this issue.

Now, expecting Congress to take up things that it might be apprised of might be asking a lot, and this is no disrespect to these incredible leaders of our congressional branch. But Congress was often asleep at the switch for many years. And the idea that we're going to trust Congress -- and you'll forgive me because I do, I've lived -- and this is no -- there are people who are very focused on it. But unless it's publicly accessible, unless it's accountable, unless it's parked at a civilian agency where the public can have access to the reports, I worry. And that's why I think that the approach that Senator Collins and the approach that congresswoman Harman and General Alexander have laid out is really the only way to begin to have the conversation.

Steve Inskeep:
How do you feel about congressional oversight? General?

Keith Alexander:
We love it.

[Laughter]

That was why our brush [spelled phonetically] as a young lad and -- actually I think it's an important thing to do. I think the oversight -- and it's not just by Congress, It's by the court and by the administration. So we get overseen by everybody. And I'm okay with that. I think it's right. You know, I just put it on the table, my experience is we have good people in the military, good people in the intelligence community, and good people in government. They are trying to do the right thing for our country. These are great people. You know, it makes me proud to server as the director of NSA. These are tremendous people. They know that everything we're doing is 100 percent auditable. We self-report. From my perspective, that's what the nation wants us to do. You know, this -- remember, our legacy -- these are the folks that helped us win World War II. So, that's the way we

look at it. We want to protect America and our civil liberties and privacy and I think we can do both.

Steve Inskeep:
Go Ahead.

Jane Harman:
Can I ask a question?

Steve Inskeep:
It's your forum.

Jane Harman:
Well, thank you. No, but we haven't touched on this. And that's about the evolving tradecraft of the bad guys: the hackers. The hackers can be individuals, they can be governments, they can be some -- industry networks, or whomever. But they're very smart. And my question, basically, is how do we keep ahead of them? Do we -- are we able to recruit people who are as smart or smarter than they are and what policies do we have to make that happen? I just put out there that I was speaking recently to the Israeli ambassador to the United States, Michael Oren, who told me that in Israel -- not that there's anything like perfect protection from cyber threats -- but they have -- they have it very well organized and they start recruiting people at age 13. And they have some kind of educational program to do this, to advise them on, you know, what this stuff is and how you identify and combat it. So --

Steve Inskeep:
Because time is short, General Alexander, go ahead. Are they getting smarter than you?

Keith Alexander:
Well, they -- yeah, we have great people. We don't have a problem hiring people today. I think the real issue is how we ensure that there are performance and pay incentives to keep them on board. That's going to be the challenge; keeping these great people in the government and in the military. And we are working at it. Right now, perhaps given where the economy is, we have don't have the problem getting the people. We have great people. What we need to sustain that -- and we -- across the next 10 years, and I think that's going to take some incentive pay like we do with foreign languages now in the cyber area, and in math and others.

Steve Inskeep:
Are you concerned at all about giving foreign actors, in effect, permission to attack the United States, or justification to attack the United States because of operations the United States may conduct overseas against various targets?

Keith Alexander:
Well I think that's where we are today. When you look at the way others can attack us, there are -- you know, the most logical way is going to be terrorist attacks and cyber. We're seeing both and we've got to get ready for those as they become more frequent. So, you know, it's much more difficult to land a division in the North, and with our Canadian allies they say we trust you to an extent -- no I'm just kidding. And so, you know it's -- we're not worried about a land attack; we're worried about missiles. We're worried about -- but the real thing -- the real way that I think people come at us are terrorism and cyber. And --

Steve Inskeep:
What I mean is the United States has cyber operations overseas, which I'm not asking you to confirm or deny, but I think about something like Stuxnet. Does that create a framework or a situation where other countries, other individuals might turn those same tactics and techniques back on the United States?

Keith Alexander:
Well I think there's a great deal -- a plethora of tools out there. You only have to go out on Google and start searching for tools and you'll find that there are thousands of tools publically available and free that could impact us today and that would impact our critical infrastructure. And so, what's going on on the network from my perspective is it's growing exponentially.

So I think independent of what you bring up that when you look at the crime and where people are going to just steal intellectual property, the way they develop those tools and the testing of those, in and of itself, brings up destructive tools. And let me more clear: When they test a tool and when they say I want to go steal something -- and so I've got this tool that takes advantage of a vulnerability than allows me access to your computer, what

they find out in executing that is, oh, it broke their computer. Okay, so that tool didn't work, but you just found a destructive tool. And so in doing that, what adversaries, hackers do in that whole scheme is grow these things. And they're out there. Some of them are for sale. You can but botnets and stuff for spam for distributed denial of service attacks, there's a lot of things out there on the network. It's amazing what's going on. So from our perspective, it goes back to the question -- the question that you had is educating our people and training them to a higher standard than the adversary.

Steve Inskeep:
Jane Harman --

Anthony Romero:
But there's one thing that I will throw a rock -- not at anyone in this room -- but it is to the hubris of this administration. If there is one thing that I fault them greatest for, is the idea that we make up for ourselves and that we break for ourselves won't be used against us. And perhaps -- certainly the quote -- the point you raised about cyber-attacks on other countries, we read them in the newspapers -- I don't have the clearance so I can't comment on it. But I can comment on the very same issue on drones. When this government uses unmanned aircraft to attack American citizens -- not in the theaters of war -- and the Chinese are not far behind us -- when I go to conferences in [unintelligible] -- you know this kind of North American-NATO get-together with people off-the-record afterwards. It's the Brits, the Germans, the Italians who all worry because they know that the Chinese and the Russians are not far behind in developing of drones. And how are we going to tell Putin or the Chinese not to use these unmanned attack vehicles when they want to go after the Chechens or the Tibetans -- it's really going to be a problem, and that's why I think that the irony of some of these technologies that we employ will come back to haunt us.

Steve Inskeep:
Because I'm a broadcaster I'm compelled to cut it off here. We could do another hour just on this discussion I think, this last bit here.

We're going to do what's basically a lightning round at the end, according to Wilson Center tradition. I'm just going

to go right across this panel and give you each a couple of sentences, a final thought to take away here. Go ahead.

Keith Alexander:
I think this is a big problem that we have. We need to educate the American people, the government, Congress, everyone on that problem. We need a team approach. And it takes all of government to help solve it, working with industry, academia, and our allies.

Steve Inskeep:
Senator Collins.

Susan Collins:
In all the years that I've been working on homeland security issues, I can't think of area where the threat is greater and we've done less.

Steve Inskeep:
Jane Harman.

Jane Harman:
I think no one should sit out this election. Even if you are sick of it in the last 37 days. And I think no one should pass up the important opportunity to get into this debate and help us fashion the right policy.

Steve Inskeep:
Anthony Romero, you get the last word.

Anthony Romero:
And I think we need -- never need to sacrifice our civil liberties in the name of national security. If you have national security without civil liberties, you have a dictatorship or a totalitarian regime. If you have safety without freedom, then you will also have an anarchy. And if you have freedom without safety, then who wants to live in that type of country where you can be free but you can't live a wonderful, free productive, healthy life? And so that's why you need both safety and freedom.

Steve Inskeep:
Okay, I feel like we've just begun the discussion, but thank you very much and please join me in thanking our panel.

[applause]

[end of transcript]