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

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 .eigwho trus sos ohe ondelo to ganotnm 0 networks bs fTD (and we're Johl

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 securasl:tiffnattackhe T*red-

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 onin

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.

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.

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 meaiskeep:

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( )Tjom]/0eMCIathre kcTj (,)Tj ( )C TD (I adD 2 >>ktr

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 wonsleah, avl/uA3MCID 0 >>BDC s -- the --

WWC: 20121001NATCON-iPhone

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

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

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

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

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:

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 Atmdings

Susan Inskeep:

One quur befororiion o kemak(analm mand Yojogy)Tave
idea liabefites.eliefildFranklj Ti222as a Anculaon the bour * (volun byt
incenti
:

incenstand rdsildSo
us a * (volunshisuldexingTtat Tinbill (enator. e, bu)we'as etailscipric

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 1.1r the h via in clud nt wn a nep- I jculd bever bTj T* (temenbersthis)orkdTj (I,Tj ( )Tj (Ibt

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.

WWC:

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

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 en tMC /P pmpD 8 >>BDC T* (An)T

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

WWC: 20121001NATCON

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]