THE ASPEN INSTITUTE

ASPEN SECURITY FORUM 2013

CLEAR AND PRESENT DANGER: CYBER-CRIME; CYBER-ESPIONAGE; CYBER-TERROR; AND CYBER-WAR

Greenwald Pavilion
Aspen, Colorado

Thursday, July 18, 2013

LIST OF PARTICIPANTS

LYNN DUGLE
Vice President,
Raytheon Company
President
Intelligence, Information, and Services

GENERAL KEITH B. ALEXANDER
Director of the National Security Agency,
Commander of U.S. Cyber Command and
Chief Central Security Service

PETE WILLIAMS
Chief Justice Correspondent
NBC News

* * * * *

CLEAR AND PRESENT DANGER: CYBER-CRIME; CYBER-ESPIONAGE; CYBER-TERROR; AND CYBER-WAR

MS. DUGLE: (In progress) have spent the day at the Aspen Security Forum, I think that there is no better way to cap off a phenomenal day that was somewhat provocative, always educational. I certainly think I speak for all of us that we're better informed than we were 24 hours ago. So as we come to this evening's event, cyber, the clear and present danger, cyber-terror, cyber-crime, cyber-espionage, and cyber-war, who better to inform us than General Keith Alexander, the director of our National Security Agency and --

(Applause)

MS. DUGLE: -- and commander of USCYBERCOM. He is the longest-serving NSA director, serving nearly twice as long as any predecessor. And in 2010, General Alexander who was feeling a little bit bored by only having one 100-hour-a-week job, raised his hand for CYBERCOM as well. And so for the past decades, and certainly the last 8 years, he has led our nation's efforts in defense and understanding and leads us into a robust discussion tonight about what the future holds.

I did a bit of a study on the general and I thought when he testified in front of the Senate Appropriations Committee, he very concisely, as he does, summarized the enormity of our challenge. He said we operate in a dynamic and contested domain that literally changes its characteristics each and every time someone powers on a network device. Make no mistake, in light of real and growing threats in cyberspace, our nation needs a strong DOD role in cyberspace.

And on a more personal note, I don't know about you, but I'm a little bit intimidated by General Alexander. Two big jobs, four master's degrees, not all of his degrees, just four master's. He can tend to be an icon. So I decided I was going to do a little of study about who he was as a human. And I tell you, I was looking and looking and I didn't think I was going to be able to come up with anything. He's a superstar in all categories.

But I got to the point where in his confirmation hearings he was talking about his family. And the general has four daughters. I don't know when you had time for that.

(Laughter)

MS. DUGLE: And he has enough grandchildren to make all of us envious. But as he went through his confirmation testimony, he talked about his wife, Debbie, who grew up -- they grew up together just two doors down, and he credited her not only for standing by him throughout his entire military career, but -- and this is the human part -- she occasionally lets him win at Yahtzee, okay?

(Laughter)

MS. DUGLE: So thank you, General, for taking time out of a spectacularly jammed schedule to join us. Our moderator this evening, Pete Williams; many of us have a date with Pete every night as we watch the news, but not everyone knows that he was previously assistant secretary of Defense for public relations at the Pentagon, and since 1993 has been the correspondent covering the Supreme Court and the Justice Department.

So General Alexander, welcome, and Pete, the floor is yours.

(Applause)

MR. WILLIAMS: Thank you very much. Let me just ask, everybody here is okay? Do we need to turn anything up or in good business here? All right, very good.

General Alexander, I typed these questions up on my computer at home. What's the answer to number five?

(Laughter)

GEN. ALEXANDER: That's classified.

MR. WILLIAMS: It's Pi over four. It's always Pi over four. Well, the President has said that he wants the nation to have a debate about these programs, so let's start right now. What are some of the misunderstandings that you have seen as these programs have become public?

GEN. ALEXANDER: Well, I think one of the things that we should start out with in answering that question, first and foremost is to put what's our mission in doing this? My mission, the mission of NSA and Cyber Command is to defend this country, that's our mission. And in order to do that we need programs that we didn't have prior to 9/11. And I think one of the biggest misunderstandings is what these programs do and what they don't do.

And this is where you and many of your colleagues can really help us out, because from my perspective the most important thing we can do is inform the American people on what these programs do. And here's a case in point. I get a lot of questions about are you reading my e-mail, are you listening to my phone calls? And you think about the volume that's out there. And the answer is with the business record FISA, and Raj De, I know, did a great job talking about this, and I would pale in comparison, but I look at it -- think of it as how you're going to do that.

How could you possibly do that and what do we need? And the answer was to solve 9/11, we needed some capabilities to connect the dots that we couldn't do prior to 9/11. And if you think that we would listen to everybody's telephone calls and read everybody's e-mail to connect the dots, how do you do that? And the answer is that's not logical. That would be a waste of our resources to get there.

And from my perspective, what you need is a way to focus on the bad guy, and if you think about it, it's like looking at one of these large-screen displays, actually like looking at a thousand large-screen displays, each one with a picture element, you've got a few billion picture elements in there, find the bad picture element. And in doing that, you've got to have a methodology for looking at the picture elements.

That methodology is to use something we call metadata. Raj gave some great insights on metadata. It's the to-from numbers to find how we can track somebody like we did Basaaly Moalin in 2007 in San Diego. It was based only on numbers, and one of the key misunderstandings is you're listening to our phone calls, you're reading our e-mails, for the American people.

That's flat not true. What we're doing is we're collecting metadata to go after bad guys who use the same devices and the same equipment that we do. They hide amongst us to kill our people. Our job is to stop them without impacting your civil liberties and privacy. And so these programs are set up to do that. And I think from my perspective we do a good job on them.

The second part is, somebody says, well, if you do this, you know, this hop thing, and I like math. Math is a good thing. Everybody at NSA, we practice math. So the first hop is 40, second hop another 40, third hop is a 40.

MR. WILLIAMS: Okay, you've lost me. I have no idea what you're hopping toward.

(Laughter)

GEN. ALEXANDER: It's like Peter Rabbit.

MR. WILLIAMS: Okay.

GEN. ALEXANDER: We'll get to that later.

MR. WILLIAMS: Let me just -- before we get into hops --

GEN. ALEXANDER: Okay.

MR. WILLIAMS: -- let me just say, what you do, you have -- talked about the phone program. You gather all this data from the phone companies, and it sits in your big tank. What can you do? Can you munch on it and chew on it and do data mining or does it just sit there until you have some specific question?

GEN. ALEXANDER: Yeah, it sits there, and that's a great question because the court restricts what we can do with that data. We can only look at that data if we have a nexus to al-Qaeda or other terrorist groups.

MR. WILLIAMS: And what does a nexus mean?

GEN. ALEXANDER: Means we have to show some reasonable, articulable suspicion that the phone number that we're going to look at is associated with al-Qaeda or another terrorist group. So we come in and as the example that --

MR. WILLIAMS: Somebody brings you a phone number?

GEN. ALEXANDER: Or we get one from our overseas collection. Remember we're a foreign intelligence agency. And I should have said upfront why are we doing this. Well, connecting the dots between what the FBI does in our country and what we do overseas, how do you connect the dots into what's getting into the United States? We see from overseas, so from some information we got in Somalia, we saw some -- we looked at a phone number, we say we know this is associated with al-Qaeda. We looked at that phone number and we saw it touched a phone number in San Diego.

And Sean Joyce, the deputy director of the FBI, was the one who said that was the Basaaly Moalin case, that they had started in 2003, but didn't have enough information to go up on. In 2007, we saw him talking to a facilitator in Somalia. We passed -- all we have is the number. We don't know who it is. We have a 9-digit number or 10-digit number. We pass that -- I guess they're 10 digits if we're going to be accurate, a 10-digit number to them and they look at that and they go, oh, this is Basaaly Moalin.

And they look up and said 4 years ago, we had a case. They reopened the case and they indicted, arrested, and convicted Basaaly Moalin for material support to terrorism.

MR. WILLIAMS: Okay, so that brings us back to hops. So somebody brings you a number, it says help us see what you can find. You find that that bad guy number that you found in Yemen or somewhere is calling a number in the U.S. Now, can you just keep going to see who that person called infinitely on, or is there some limitation?

GEN. ALEXANDER: There is a limitation by the court, and there is a logical limitation. And so the other one that we publicly released was the Najibullah Zazi -- and I practiced all day to say that one.

(Laughter)

GEN. ALEXANDER: Local boy. Local boy. We call him Mr. Z. This was another case like that and it gives you the hops. And I think it's important to discuss this because it puts into perspective a fallacy that's out there. So remember, our job is to help the FBI, tremendous partners. You know, Bob Mueller and his team are absolutely superb and we're losing a great individual as he retires; 12 years he's had.

Now, Najibullah Zazi, we were tracking an a-Q operative in Pakistan. We saw this communications on a recipe for building something that looked like a bomb to a guy, an e-mail address. We gave that e-mail address -- and inside there was a phone number, but we didn't know if the phone number was U.S. or foreign -- we gave that to the FBI. The FBI took that and said, this e-mail address goes to Najibullah Zazi and that's his phone number that was in the message. Based on that, knowing the nexus now, reasonable, articulable suspicion to al-Qaeda, we are now authorized to hop and see who is Najibullah Zazi talking to and what are they planning.

The first hop was to a guy named Adis Medunjanin in New York City. The second hop was to a group called Op Wi-Fi, another operational group, and the third was to the Raleigh-A (phonetic). Now, the FBI was getting information on that same guy in New York City. This is in September of 2009 and they were going to conduct an attack in mid-September. And based on the way this moved Customs, Border Patrol, our support, the tip -- if it was not for the tip from FAA 702 that we gave, the FBI would not have seen that, and they would have hit the New York City subways.

That would have been the biggest event in the United States since 9/11 stopped by one of these programs and the great work by FBI and other agencies all working together.

MR. WILLIAMS: So what is the limit on the number of hops you can take?

GEN. ALEXANDER: So we're limited to three hops, but there is a logical limit. And I know somebody is doing the math, this gets to 40. Somebody used 40 times 40 times 40. Big number, 64,000 I think it is. Check that. Okay, and then they went another hop. They went a fourth hop. We can't do that. And they go to 2-1/2 million. But think about this, our intent of doing the hops and looking for this is not to see how many numbers we can give to the FBI to see how long we can have them spend looking at numbers in a very sensitive investigation.

The intent is to get this down to the right numbers that matter. So if we gave them 64,000 phone numbers and said, hey, go look up these --

(Laughter)

GEN. ALEXANDER: -- they would think we're idiots. We would prefer that they don't think that.

(Laughter)

GEN. ALEXANDER: So what we do is we winnow it down and we say here are the ones that seem to matter, and then they can -- remember, they had about 7 days to break this case. Think about that. They are already moving from Colorado to New York City, had 7 days to break it. If we gave them 64,000 phone numbers, said good luck with that, we're not helping. Our job is to help. The metadata program is designed to help connect the dots between what we see foreign and what we see in the U.S. without U.S. person's name or content. It's metadata. The phone number to and from, the duration, and date-time of the call.

MR. WILLIAMS: So Edward Snowden has said in these interviews, some of these interviews he's done that he had the capacity to -- if he wanted to, he could listen to the President's conversations or anybody's he wanted. Can you do that?

GEN. ALEXANDER: No, we cannot. And you see, so those are some of the fallacies that are out there that, you know, we don't -- one, we don't have the technical capabilities. We're a foreign intelligence agency. To do that, you'd have to have the -- you know, you'd have to have AT&T and everybody else's networks and we don't. We'd have to go to them and I know one of the things that you look at is with these servers we don't own and operate AT&T. We couldn't compel them to listen to those phone calls. That would require a warrant and probable cause finding. And under the FISA thing, we wouldn't have a reason to do that. That would be in FBI. You couldn't sit at my desk at NSA and do that. Couldn't possibly do it.

MR. WILLIAMS: So you have said that the disclosure of these programs is damaging. But explain something to us. I mean, we know that Osama bin Laden was so worried about having his communications intercepted that he used couriers. So surely the bad guys know that we have the capacity to listen in on their phone calls and read their e-mails. How can the disclosure therefore of these programs be so damaging?

GEN. ALEXANDER: Well, it's our tactics, techniques, and procedures for going after them. And what we're doing is every time we talk about this, we take what I think are the most important tools that we have in our first line of defense for defending this country, and what we're doing is we're telling them here's our playbook, here's how we're stopping you, perhaps if you tried a different method, you'd be successful. And that's just plain crazy.

What we're doing is irresponsible in this area. And I think it's significant and irreversible damage to our nation. And we've got to be clear on that. The purpose of these programs and the reason we use secrecy is not to hide it from the American people, not to hide it from you, but to hide it from those who walk among you who are trying to kill you. How do we do that? That's part of the debate.

How do we protect you and your civil liberties and privacy and still get the terrorist? And the answer can't be, well, we'll just tell them what we're doing because what they're going to say is, okay, now we know.

MR. WILLIAMS: Well, have you seen any evidence of that?

GEN. ALEXANDER: We have.

(Laughter)

MR. WILLIAMS: So you have seen --

(Applause)

MR. WILLIAMS: Well, what sort of evidence have you seen?

(Laughter)

MR. WILLIAMS: So to be clear, you have seen concrete proof that maybe places where you used to be able to listen to are now silent?

GEN. ALEXANDER: We have concrete proof that they have already -- terrorist groups and others are taking action, making changes, and it's going to make our job tougher. And here is what really hurts. And you know, we have some great warriors sitting in the front row here, Carter Ham, and Bill McRaven. Let's give them a big round of applause.

(Applause)

GEN. ALEXANDER: Two guys in Iraq and Afghanistan, both of them. We had the honor and privilege of supporting them. And the whole role of NSA was to defend in those cases our troops abroad. And what they did to take care of our troops and defend our nation was extraordinary. These tools are critical to defending them. And what we're doing is telling the enemy our playbook.

There is reasons we keep this secure, and it's not because we don't trust you. If we could just get all the American people in our huddle and say, okay, here is the game plan, we would do it. But the reality, terrorists use our communications devices. They use our networks. They know how to plan around this. They use Skype. They use Yahoo. They use Google. And they are amongst us and they're trying to kill our people.

And as was mentioned, I have 15 grandchildren. I want to make sure they're safe. They're our future. And we ought to -- that's something that we lived through in 9/11 and we said, never again. And what we have from my perspective is a reasonable approach on how we can defend our nation and protect our civil liberties and privacy. And so if you think metadata, think about the numbers that we went into in 2012. Less than 300 selectors were looked at.

MR. WILLIAMS: What's a selector?

GEN. ALEXANDER: Selector, phone numbers. Think of that as the number. So we had less than 300 selectors approved for 2012 to dip into that database. That's a very focused effort. It's based on a nexus to al-Qaeda and terrorism. It's exactly what you would want your government to do.

MR. WILLIAMS: And be clear, last year you only dipped into your phone number tank 300 times? Is that what you're saying?

GEN. ALEXANDER: No, I'm saying that we had numbers that allowed us to dip in, and then we would dip in on that number and see if anything just changed periodically based on the requirement of what that number is. And we would do one, two, or three hops based on what we thought from the mission perspective was needed. And we issued a few dozen reports to the FBI. So a very focused program meant to connect the dots between the foreign intelligence agencies and the great FBI. And John Pistole there was the deputy director and a great partner.

MR. WILLIAMS: So one of the questions is, you know, who needs to keep the data? Whose tank is it? It's yours right now, but why not let the phone companies keep it? Let me ask you this question. Juan Zarate and Leonard Schrank wrote an op-ed in the *New York Times* recently about how the Treasury Department does this with bank metadata. And in that case, it's the industry that keeps the data, and when the government wants it, it goes to industry which has combined all the banking data put together. So could you do that with the phone companies, say you guys keep all this and when we need it, we'll come to you?

GEN. ALEXANDER: And I know Dennis Blair talked about this earlier today, but you could technically do that. Now, it creates some operational problems that we'd have to work our way through. Specifically you would have some data over here, some data over here, and some data over here, and if you queried it and you got numbers that touch over to this database, you've got to pull out -- touch to this database, go back to this database, and you have to iterate through that. So it would --

MR. WILLIAMS: Well, but I'm thinking of something like the Swift (phonetic) database which is, you know, all the phone companies together form a consortium for example and put all this stuff in, but it's their tank and not yours.

GEN. ALEXANDER: So what we do is move the wire a 100 miles down the road, and that may be the best solution if you could come up. But you'd also have to change the legislation to require them to keep it, and then have them keep it. And so then the issue is so how many people now have access to the data, and how does the court oversight go to that and how do you do that? Those are things that would have to be looked at. And these are actually issues that both the House Intel Committee and the Senate Intel Committee have asked.

So they're looking at the same thing, is it possible? What's the cost, and what's the operational impact? Now, as Dennis Blair said, we talked to the phone companies in 2009 and they said, okay, we prefer not to do that. Now, we could work that, I'm sure the government could come up with some way of working that with the companies. I think it's something that we should consider. I'm not against it.

MR. WILLIAMS: If there -- I mean, I suppose the government would, number one, have to require them to do it, and number two, pay them to do it. But if it did, and if that made the American people somehow feel better about the fact that it's not the government that has those numbers, operationally, from your perspective, would that be a problem?

GEN. ALEXANDER: Not operationally if you had the data in the same establishment that we have right now, no. Now, there's one other thing that we should put in here. Everything we do is a 100 percent auditable. So every time we make a reasonable, articulable suspicion, we have to document it, and then all our oversight committees can look at do they do it right, from the courts, Congress, and all sorts throughout the Executive branch. So no matter what we do, we'd still have that level of oversight so that you know that what we're doing is being audited by those committees, by Justice, by the courts, so that everything that we're doing is exactly right.

And oh, by the way, none of this has been about us doing something wrong. It's not that we're doing something that's outside what we've been asked to do. We're doing what we've been asked to do, yet we do make mistakes. If we do make a mistake, we tell everybody in that chain what we did, what we're doing to fix it, and if it's with the court, the court hauls us down there, we have a discussion. And many of you may have been in front of a federal judge before. It's not a pretty scene.

(Laughter)

GEN. ALEXANDER: And for those who said that was rubberstamp has not been in my shoes when we make a mistake. So I would tell you, I think if the American people could sit from where we sit and see how this was run, they'd say that's exactly what you should be doing. And I think it's the right thing to do. And you know, when you think about it, 300 numbers in a year, it helps stop -- we are going to talk about, you know, how many -- well, look at how many this helped stop, how many terrorist activities; 42 different plots, 12 times we caught people, material support to terrorism; 54 that we pushed out, 13 in the U.S. And the only ones in the U.S. are the only ones that BR FISA could help on in 12 of those 13 BR FISA had some role whether it was to help or to show not.

MR. WILLIAMS: Let me ask you about that number if I may. So 54 plots you've talked about, or terrorist events I think is the phrase you used. In how many of those cases was it the phone program that was the red light, and in how many of those programs was the initial tip from the other program we haven't talked about as much, which is the Internet program?

GEN. ALEXANDER: So FAA 702 is the other program. That's the one, foreign, reaching inside based on a certification that this is for example CT, counterterrorism or others, that allows us to compel the carriers to go after it. We can come back to that point in a minute; 53 of 54, the FAA 702 played a role in. BR FISA, or the business record FISA are metadata can only apply to the ones in the U.S. and there were only 13 inside the U.S. It applied to 12 of those 13. Now, you asked a great question and the answer, this is like putting together a puzzle, the dots. And what we're trying to do for the United States is to provide that information to the FBI.

And what you can't afford to do is what we did in 9/11, not have enough information to connect the dots.

We all came together as a country and said never again. We don't want another 9/11. And look at the track record since 2001. It's extraordinary what the FBI, CIA, NSA, Defense Department has done to protect this country is absolutely amazing. And one more thing for the American people from my perspective, 41 of those were with our allies; 75 percent of the time we helped defend them with these programs. Germany, France, Denmark, and other countries around the world benefited from what the United States did here.

And from my perspective, that lawful program that we have under court supervision is run better and has better oversight than just about any other country in the world.

MR. WILLIAMS: But you mentioned the Zazi case earlier, and you say that the breakthrough there was seeing that he is e-mailing the bad guys saying, you know, remind me again how do I make this bomb. And that's what then is the initial tip that leads to the phone numbers. So up goes 54 cases that you've mentioned. In how many was the e-mail program the initial tip-off? And in how many can you say was the phone program the tip-off?

GEN. ALEXANDER: Yeah, I don't have the numbers off the top of my head to break it out like that, but clearly the FAA 702 with content based on knowing that's the bad guy has then --

MR. WILLIAMS: And that's the e-mail program?

GEN. ALEXANDER: That's the e-mail program, is much more effective in that regard, and the business record is starting back a step. And so let me clarify this so -- to help all of us understand what we're talking about here. The first step is if you don't know who the bad guys are, it's hard to go collect their e-mail, right? So you can't take the first step in going after Zazi if you don't know he's a bad guy.

So you need a program using metadata analysis to find out who the bad guy is. If you try to just collect everybody's e-mails, you know, let me go ahead and read them all, one, we'd have to have mega reading classes a lot and it would be operationally inefficient and ineffective to do it. So what you need is a metadata program to steer it. What that means is we're a foreign intelligence agency. Our job is to go after foreign intelligence requirements. We don't listen to the people, phone calls in Brazil just for fun, or read their e-mails, it would be operationally ineffective to do that, nor do we do that in Germany.

What do we do in Germany? Well, the counterterrorism is a great case in point. If we see a terrorist trying to get into Germany, we use a metadata to figure out who it is, we pass that to the German authorities. And if we got it from the FAA 702 and it's relevant to that, we pass that to the German authorities. And you need those programs to work together because you can't do -- look at the billions of e-mail and the number of calls. It would require way more people, millions, hundreds of millions of people to do that.

We could not possibly do it. And so I think -- you know, this is where I think in this debate one of the things that we could do is help educate and inform the American people on this. And this is where -- we have some of the best press people in the world in this audience. Don't raise your hands.

(Laughter)

SPEAKER: We all would. We all would.

MR. WILLIAMS: One of them is right here.

GEN. ALEXANDER: So my comment is, look, think about the math in this. Think about what we're trying to do. Help us defend this country and protect our civil liberties and privacy. And if anybody has a better way to do it than what we're doing, we are -- we want to hear that.

MR. WILLIAMS: Let me ask you about -- a question, you talked about your industry partners here, so today, Apple, Google, Facebook, LinkedIn, Yahoo, Microsoft, Twitter, and several other computer and communication companies wrote a letter to the administration -- one copy to you -- saying they want the legal authority to be able to publicly disclose the number -- the scope and number of requests they get from you to disclose information. Would you be in favor of that?

GEN. ALEXANDER: Well, let me hit a couple of things. Yes, but I want to caveat that. First, these carriers are compelled to support us in these programs. They don't have a choice. Court order, they have to do this. And you know, these are global companies. They are oftentimes compelled if they have a headquarters in another country to do the same thing, a lawful intercept program, they have to do that. Now, from my perspective what they want is the rest of the world to know is we're not reading all that e-mail, so they want to give out the numbers.

I think there's some logic in doing that, and the issue really comes down to these programs -- there's two general fields for getting this, one is for criminal law enforcement the FBI runs and one is the national security side of that. And so the FBI -- and we are trying to figure out how do you do that without hurting any of the ongoing FBI investigations. So that's the hard part.

But the reality is when you look at the numbers and people look at that, they say, okay, this is a logical and reasonable program. So they're working their way through this. We just want to make sure we do it right, that we don't impact anything ongoing with the FBI. I think that's a reasonable approach. From my perspective, what the American people and the rest of the people in the world should know, what these companies are doing -- they are compelled to do, and I will tell you, they know that they're helping us save lives here, and in other countries around the world, and that's good business because there's more people who can buy their products.

(Laughter)

MR. WILLIAMS: This program is supposed to be about cyber, and don't worry, we'll get to that. But I have a couple of other questions about things that have arisen since this program was set up and the program was printed. Let me ask you about Edward Snowden. I realize you can't tell us what he got, but do you feel now that you know what he got?

GEN. ALEXANDER: Yes.

MR. WILLIAMS: And was it a lot?

GEN. ALEXANDER: Yes.

MR. WILLIAMS: How did it happen? Didn't you learn your lesson from the Bradley Manning case that people aren't supposed to be able to plug stuff into your computers and just download it?

GEN. ALEXANDER: So the issue here is many of you may already know that this leaker was a system administrator and ran the SharePoint account in NSA, Hawaii. And so his responsibility was to move data. And as a system administrator he also had access to thumb drives and other tools. So what we had is a person who was given the responsibility and the trust to do this job, betrayed that responsibility and trust, and took this data. Now, I know Dr. Carter talked about some ways of doing it, two-person rules, what we can do within DOD, what we can do across the intelligence community. We're taking the actions to fix this.

MR. WILLIAMS: So what does that mean practically, that no one person can move a file, it takes two to do it?

GEN. ALEXANDER: And you limit the numbers of people that can write to a removable media, instead of allowing all system administrators, drop it down to a few, and use a two-person rule. Look close, and lock server-rooms so that it takes two people to get in there. This makes our job more difficult. It is the main reason we need to jump to the Joint Information Environment, the thin virtual cloud, because in that we can also then encrypt the data and ensure if somebody were to steal it, it's encrypted.

I think we also have to ensure that we make sure that people who need information to do their job have access to that information. That was one of the lessons learned, so we want to balance these two and get it exactly right. So we have that. That's one of our jobs to fix. Since this happened at our place on our watch, we're piloting that for DOD and for the IC, and we will fix this in our stuff. That's our responsibility and we will do that.

MR. WILLIAMS: Do you have a way of distinguishing between what Edward Snowden looked at and what he actually downloaded and took? Do you have a pretty good idea of what he downloaded and is there some order of magnitude you could tell us about was it millions of documents, hundreds of thousands?

GEN. ALEXANDER: I really can't go into that because that gets into the law enforcement side, and that's over in the FBI channels right now.

MR. WILLIAMS: But what about the other part? Can you tell the difference between what he looked in the library and what he actually checked out?

GEN. ALEXANDER: We have good insights to that, yes.

MR. WILLIAMS: Okay. Let me ask you about a comment made by a U.S. senator earlier this month. Let me quote what he said at a hearing. He said, "We have heard administration officials defend programs like the one we've been talking about by saying that they were critical to identifying and connecting the so-called dots. There's always going to be more dots to analyze and collect and try to connect. When government is collecting data on millions of innocent Americans on a daily basis, when is enough, enough? Just because we have the ability to collect huge amounts of data, does it mean that we should be doing it?" So when is enough, enough, or would you always want more?

GEN. ALEXANDER: Well, I think the issue is what does it take to stop a terrorist attack. I mean this is the real issue because we're not playing in this data to just while away our time. What we're trying to do is find out what the terrorists are doing. What we're doing is defending our troops forward. We're trying to defend this country. And what we know from 9/11 is we didn't have enough information to connect the dots. We know that these two programs have helped us do this.

We know that the damage caused by this information going out is significant and irreversible and will make it more difficult in the future. But from my perspective, what we don't want to do is start saying, well, let's cut back a little bit and see where the edge is, and say, okay, a terrorist attack, okay, step forward one step. It's not like that. When you look at what we're asking the FBI to do to defend this nation against terrorist attacks, time is of the essence. Sean Joyce did a great one at the 16th June, and I don't have it here with me, I know I was supposed to memorize it, but you know, what's the value of a American citizen? It's priceless.

That's our friends. That's our family. That's what we vowed to take care of. That's our job, is to defend this nation. And what we're not asking is for data that we're just going to troll through, it would be illegal, but we do need the information to protect this nation. And we have more oversight on this program than any other program in government that I'm aware of.

MR. WILLIAMS: So let me just say as a program note here, we started about 5 minutes late. So I'm just going to go about 5 minutes longer. And if anyone here tries to stop us, there's a guy in uniform next to me, good luck with that.

(Laughter)

MR. WILLIAMS: There was a fair amount of discussion here today about relevance, because the law that allows you to get this phone data says you can order companies to turn it over if it's relevant to an investigation. And the question has arisen several times here today, how can every phone record in possession of a telecommunications firm be relevant to an investigation? What's your answer to that?

GEN. ALEXANDER: So the issue is what you can do is if you don't know who the bad guy is, so let's say you have a million dots on the screen and you're not allowed to collect any until you have a problem and say, okay, I now have a question. And somebody says, what's the question? I have this number and say, you didn't ask about that number, we don't have anything on that number. Well, why not? Well, we didn't keep it. Well, why not? Well, we didn't know it was relevant. So we argued that, the courts argued that, Justice argued that, and said, well, so you need the data, you need the haystack to find the needle. If you don't have it, when you go to ask it, it's not going to be there.

MR. WILLIAMS: But this answer seems like the old gag about the guy who has lost his watch and someone says, why are you looking here? He says, well, I lost it down the street, but the light's better here. I mean --

GEN. ALEXANDER: No, that -- in fact it's just the opposite.

(Laughter)

GEN. ALEXANDER: And what it's saying is, if you only look under the light, you won't find your watch. And if you only go with the numbers you know, you won't find the 9/11 guys in it because you didn't know about them. So how do you find Midar in California? And the answer was, shoot, we didn't have his numbers, we didn't have the numbers to look at. We didn't have a database to go. We needed that database. And so that's why we put this together, to solve the Midar case. And --

MR. WILLIAMS: Well, from a legal perspective, is the government basically saying that it's okay to gather this stuff, and it's -- you should only be concerned about it when we actually look at it. We should think about this in terms of when you look at it rather than when you gather it?

GEN. ALEXANDER: Well, I think that's where the court puts restrictions on how we use it. So what the court said is, okay, we agree with the findings from Justice, they've gone through this and they looked at it, but they said, here's some restrictions. One, you can't just go through the data and do all the stuff that everybody believes we're doing. You can only look at the data when you have a phone number, a number, reasonable, articulable suspicion that it's associated with al-Qaeda or terrorist groups. And then and only then can you look into that. And you can't do it for drugs, you can't do it for other problems that you come up with, only for that case because that's the way the court designed this, and the way the Justice worked it.

So from my perspective it's to address this problem and I think when you look at it, and you look at the safeguards that go into it, and you think about the numbers, think about picture elements in a thousand different large-screen high-definition TVs, find the right picture element. It'd be impossible to do without some program on it.

MR. WILLIAMS: One other question about how legally to think about this. What if the police said, you know, we have a problem. People are selling drugs in this neighborhood in Aspen, and so what we want everybody to do is just -- we're going door to door and have you empty your pockets. And then we'll put that in a big box and if there's ever a drug investigation then we'll look in the box. But trust us, we won't look until we need it. Why shouldn't we think of the phone program as like that?

GEN. ALEXANDER: Well, for one there's the 1979 Supreme Court case that looked at metadata. And I know you guys discussed that and I know that Raj discussed that earlier, so I won't go through all that. But there is --

MR. WILLIAMS: But that's the case that said there's no reasonable expectation of privacy in the records you give a phone company?

GEN. ALEXANDER: Exactly right. And it also means that it doesn't then go into the unreasonable search area. What they've done is to make sure that what you're doing is correct, is limited, how you look at the data and when you can look at it. And that's where the reasonableness comes in. So from my perspective, let's look at it this way.

You know, from us, from America, from our perspective, how could we better stop terrorist attacks? What more could we do to keep this country safe? We all lost friends and other citizens in 9/11. We made an agreement that that wouldn't happen again. And what we're doing on this, less than 300 selectors in a year, I think is reasonable and proportional to what we need to do to defend this country. And with the oversight that we get from the courts, Congress, and the administration, I don't think we could ask for anything better. I think everybody who has looked at this has said, yeah, when you look at it, it's the right thing.

So I do think from my perspective, this is the best approach. Now, if somebody comes up with a better idea, we want to hear it because reality is, the job is to tip the FBI to catch bad guys, stop terrorist attacks. That's the mission here, and help our allies.

MR. WILLIAMS: Let's move on to cyber and I just have a couple of questions and then we'll invite questions from folks in the audience. We've heard a little bit earlier today from Ash Carter about the fact that you all are ready to start deploying cyber teams to be able to carry missions out. Can you tell us a little more about that and what are these teams supposed to do? Are they merely defensive or will some be offensive that can stage a cyber-attacks?

GEN. ALEXANDER: It's both, both offense and defense. And we are biased towards defending our networks and the nation, first. That's our first mission. And so the teams that we're standing up first are ones that would defend this country and defend our networks. And I think Ash Carter talked about that briefly. Let me give you some insights. Look at what happened to Saudi Aramco in

August of 2012. The data on over 30,000 systems was destroyed; and then in RasGas in Qatar, in South Korea in March and again in June.

These are destructive attacks. And we've had hundreds of attacks against Wall Street distributed denial of service attacks. It's getting worse. They are impacting our nation's financial sectors, going after energy and stealing intellectual property. We have to work together as a nation to solve this. We absolutely have to do that. Our job, U.S. Cyber Command's job, and NSA's job is to work together to provide the capabilities to defend this country, to defend the DOD networks, and to work with DHS, FBI and others in the defense of this nation. And I think actually we're doing pretty good on that.

We are standing up teams. We're training them and certifying them all to a standard. I think just as you would want us to do, they are going through that training, they will be certified. We'll know that what they are doing, they are trained to the right standards to do this, a huge step forward. It's going to take time. The service chiefs, I know Mark Welsh was here yesterday, are bending over backwards to help push units into this. They realized that there is a couple of areas that this country has its risks, terrorism, cyber and we've got to be prepared for those. And so we're doing a lot in that area and I think standing up these teams, the work is going good. We've stood up several teams.

MR. WILLIAMS: How many?

GEN. ALEXANDER: Several.

MR. WILLIAMS: Okay.

(Laughter)

MR. WILLIAMS: More than three?

GEN. ALEXANDER: Yes.

MR. WILLIAMS: Okay. Do you -- are the rules of engagement clear for the offensive teams, when we shoot first?

GEN. ALEXANDER: Well, the -- so the shooting first is a policy decision. What we do is train, just like any other military outfit. We train these folks to do what they need to do to defend our country. And you know, for defending yourselves it's not just catch bullets, I'm just thinking out loud. If somebody is shooting a missile at you, you don't say, okay, I've got to catch this one, I wish I could shoot it down. You might want the capability to shoot it down.

And in cyberspace, you're going to want the same capabilities to stop somebody from taking down Wall Street. We're going to need capabilities to do that. You would expect us to have those capabilities. But the decision to employ those is a policy decision. Our job is to set those up, and what we will be capable of doing and authorized to do is to defend within our networks. And to raise the issue to the secretary of Defense and the President and say here's the issue that we see, over to you for a policy-level decision.

MR. WILLIAMS: All right, let's take some questions. There is somebody roaming among you.

GEN. ALEXANDER: Could I hit one other thing.

MR. WILLIAMS: Yes, please.

GEN. ALEXANDER: I just wanted to hit one other thing, cyber legislation, if I could.

MR. WILLIAMS: Yeah.

GEN. ALEXANDER: We do need cyber legislation. Why? We can't see Wall Street as an example.

MR. WILLIAMS: What does that mean, you can't see it?

GEN. ALEXANDER: Well, from Aspen it's a long ways away. No, actually --

(Laughter)

GEN. ALEXANDER: -- in cyberspace --

MR. WILLIAMS: On a clear day, you can see Wall Street.

GEN. ALEXANDER: That's right, on a clear day, but you've got to stand up on that mountain. In cyberspace, we can't see somebody attacking Wall Street from Wall Street's perspective. So if somebody were to employ a destructive attack, somebody's got to tell us, call us. We're standing by the phones, you've got to tell us that. But how do you work that?

Companies can't share some of that data with the government. We need legislation to work with the government, between FBI, DHS, NSA and Cyber Command, we need them to be able to tell us and we need to tell them what the bad guys look like. Think of this as cars on the highway. If you see a red car on the highway carrying explosives, please stop it, tell us where you saw it coming from. If it's overseas, NSA Cyber Command will work it. If it's in the United States, DHS, FBI will work it.

But we have to have legislation to get us working together. And if we do that, we've got to figure out how to set the right liability protections. I don't know what those are, I know folks are working that from the White House and in Congress. We'll get that right, but that's what we need.

MR. WILLIAMS: Why do they need liability protection, protection from what?

GEN. ALEXANDER: Well, for a couple of things. If we tell them it's the red car, and the way we stop the red car, also stops red-striped cars by mistake because the government makes a mistake, then the government should be accountable for that.

MR. WILLIAMS: Okay, questions. Right here, yes sir. Wait till the person -- oh, there is -- well, yes, right as I said. Right there.

MR. BELL: Clark Bell of McCormick Foundation. Were you surprised at the extent of the backlash post-Snowden?

GEN. ALEXANDER: I was, partially because I felt that the way the information was put out there didn't set the right framework for it. So the way it first came out is NSA is in all the systems, got on all the servers and getting all this and listening to all your phone calls. You now know that's not true. It's absolutely not true.

But that's how it started out. So what we did is we raced to the wrong conclusion and started this debate. If we're going to have a debate, let's have it with the facts. I do think this is a good thing to do. There is risk in having a debate on a national security issue. The adversary will learn what we're trying to do. So there are some things that we can't share. And I think the American people have to understand that the Executive branch, the courts and Congress, your elected representatives are going to do the right thing here. And from my perspective, on our intel committees and across the board, they are doing the right thing. So yes, I was.

MR. WILLIAMS: Right there, yes sir.

MR. O'HARROW: General, I'm Bob O'Harrow at the *Washington Post*. I'm interested in the fact that earlier today Deputy Secretary Carter said that -- he called it a major mistake to put such large pools of information together while giving access to that information inside the NSA to a far wider variety of people than may have happened a generation ago. That's what I guess some people call the insider threat or the insider cyber-threat. You addressed that briefly earlier, but how big is that threat both inside the government and in corporate America?

And what -- can you give us a little more detail about your efforts to fix it? And finally why is that threat still in place after Buckshot Yankee and WikiLeaks earlier?

GEN. ALEXANDER: Well, so each one slightly different. Starting at your last question first, this leaker was a system administrator who was trusted with moving information to actually make sure the right information was on the SharePoint servers that NSA Hawaii needed. A huge break in trust and confidence. So there is issues that we've got to fix there.

I think the second part of that is what do system administrators need access to and how do we limit that, what do our analysts need access to and how do we limit that. And I know John (phonetic) is -- John -- one of the premier guys from another agency with great analytic experience knows that if you don't give the analysts the right information, you know, that's -- so we've got to figure out how to balance this. I am a tremendous advocate for the Joint Information Environment.

I know Dr. Carter perhaps didn't get the time to talk about that, but that's where we need to get to. And the reason is, then all the datasets could be encrypted differently and those who have a need for that dataset can get access to the dataset and only the datasets they have -- they need access to. Now, after 9/11 we had this need to share. I think there is goodness in sharing.

We've got to make sure that we do it right. I think we've got to stop people from being able to download information including system administrators while we go to the two-person rule, and while we lock down the server-rooms. Those are the key things that we will do to address this. But as you may know, system administrators need removable media to do their job. That just makes our job twice as hard now.

MR. WILLIAMS: Question from the gentlemen from ZDF here.

SPEAKER: Would you please --

MR. WILLIAMS: Wait till you get the microphone here or speak extremely loudly, one or the other.

MR. BERRY: Stephen Berry, the University of Chicago. Could you say something about the current manpower situation for the capability to maintain cyber security? This is certainly an issue that we face right now.

GEN. ALEXANDER: So there is a tremendous set of issues on manpower. So one of the reasons Secretary Gates made the decision to put Cyber Command at NSA is to leverage the technical capabilities that NSA has. All those mathematicians, computer scientists, the real technical people who worked on the networks every day, we need to leverage those. And to create with the military the Force structure we need to support combatant commands to defend this nation and defend the DOD networks.

And if we put those two together and came up with a training program, think of this just like you do at the University of Chicago, what you're doing is you're bringing in folks to train and you're using the great staff that you have there like Dr. Grossman and others to train these people. And from our perspective, we want to do both just as well. And I think that's a great step forward.

So we don't need everybody to be at a master's degree level to operate in this space. We can train some of them, and you know, some of the young folks we have coming into the military are absolutely superb. And we can't train those, but we do need people up here who have a Ph.D. in mathematics, a Ph.D. in computer science. So NSA can do parts of it, Cyber Command can do parts of it.

Now, this is going to be a challenge to keep those folks. That's going to be a real issue. And so we've got to look at how do we incentivize soldiers, sailors, airmen, and marines and we're looking at that, because I do think that's very important. And I'll come back on the people of NSA at the end. I just got to make sure I do that. Thank you.

MR. WILLIAMS: Well, let me ask you right now, what sort of impact has all of these leaks and the public debate had on morale?

GEN. ALEXANDER: Well, it's impacted it for a couple of reasons. You know, the great question from the *Washington Post*, we're a great technical agency. To have this happen to our agency is just flat wrong. You know, we have great people and you know, I was -- I'm glad that both Carter Ham and Bill McRaven are here, because two of the folks that we had the honor and privilege of supporting in Iraq and Afghanistan are here.

We take supporting our folks abroad and defending this country to heart. Our people look at that as a privilege and honor to serve this country. They serve in silence. We have great support with FBI, CIA, the rest of DOD and we operate as a great team. And you know, when I look at that, we've had 20 cryptologists killed in Afghanistan and Iraq since 2000 -- since we started those. These are folks who gave their lives to ensure that our troops would come back.

They are the ones that helped defend this country. They are the true heroes in this, make no mistake about it. These are great people who we're slamming and tarnishing, and it's wrong. And it ought to stop. And you ought to help us get that word out. They are the heroes, not this leaker and others. What they're doing --

(Applause)

GEN. ALEXANDER: And I'll tell you I couldn't be more proud to work with those folks. It's an honor and privilege every day.

MR. WILLIAMS: Okay. Question right over here. Yeah, right there. You've got the microphone. Oh, you brought your own. How nice.

ZDF German TV: Actually I just got it. Thanks, Pete. Alma Tevison (phonetic) with ZDF German TV. Thank you, General, for sharing your thoughts with us. You mentioned Germany of course. How big of a surprise was it for you that German politicians and German authorities claimed so much surprise about the extent of the programs?

Didn't they know all along? And while I'm at it, I also have a second question, why you're focusing so much in gathering data also from Brazil since there is not too much terrorism going on in Brazil as far as I know.

GEN. ALEXANDER: So two questions. First, every nation acts in its own self-interest, Germany, France, the United States, Brazil. We all have intelligence agencies, and I'm sure they're doing something.

(Laughter)

(Applause)

GEN. ALEXANDER: Inquiring minds want to know. You have great intelligence agencies and great people there. It's an honor and privilege to work with them and to stop terrorist attacks and for what they've done in Afghanistan, absolutely superb. But we don't tell them everything we do, nor how we do it. Now they know. And they know that our programs, that we do go through a court process that's probably more rigorous than anybody's in the world.

And Brazil, you know, the reality is we're not collecting all the e-mails on the people in Brazil nor listening to their phone numbers. Why would we do that? What somebody took was a program that looks at metadata around the world that you would use to find terrorist activities that might transit and lead to the conclusion that Aha, metadata, they must be listening to everybody's phone, they must be reading everybody's e-mail.

Our job is foreign intelligence. I'll tell you 99.9 -- and I don't know how many nines go out -- of all that whether it's in Germany or Brazil is of no interest to a foreign intelligence agency. What is of interest is a terrorist hopping through or doing something like that. So ours has to be based on a foreign intelligence requirement.

What has been grossly misstated is that we're reading everything. So what I would ask you to do, just look at the numbers of people in Brazil, 201 million, and

I got that -- I googled that today --

(Laughter)

GEN. ALEXANDER: -- just wanted you to know, 80-some million in Germany. Think about the amount of e-mail and phone number data that it would take to do that. And I was talking to one of our European partners whose name we won't use, and their comment is if we wanted to do that, half the country would have to be listening to the other half.

(Laughter)

GEN. ALEXANDER: And it's not possible and it doesn't make sense. And if you think about it, think about what you need to do to actually find the right people to go after. And there is enough bad guys to keep all our intelligence agencies busy. And so I think what we need to do is get the facts out. By alarming people and say they're reading all your e-mail, they're listening to all your phone calls, you know, it's wrong, it's absurd. And so that's where I think the newspaper people in here could do a quick study, think about how hard that would be and step back and say does that make sense, and the answer would be, no.

MR. WILLIAMS: Questions over here. Josh.

MR. GERSTEIN: Hi General, Josh Gerstein with *Politico*. You know, all these programs involved some kind of tradeoff. I think you'd acknowledge that say with the phone call database there is some intrusion. The President has acknowledged there is some intrusion on people's privacy to collect all their phone numbers. So we have to judge whether that intrusion makes sense.

My question is why can't you guys come up with a better example of where the phone call tracking database program has been useful? You mentioned this San Diego case, Al Moalin or something to that effect, which as I understand it is, he was a -- someone involved with al-Shabaab, which is a bad news organization I think most Americans would agree, but it seems a pretty far cry from a domestic terrorist event that people would be acutely concerned about. And then when pressed further, you revert to the 702 program and Zazi and New York which everyone would be greatly concerned about, but I don't understand the connection between that and collecting everybody's phone numbers. So can you explain a little bit with the dozen cases you mentioned why we don't have a better example?

GEN. ALEXANDER: Sure. So the Zazi case, there is two parts to it. And thanks, because I do want people to understand this. The Basaaly Moalin was done all on business record FISA, all based on the metadata program, all tipped from that. So that's one. But to really understand the value of it, it's not that these are going to have or stop that, these are going to present capabilities and insights for FBI to put together the puzzle to help them understand what's going on.

And the Zazi case is actually a case where you're starting to bring in multiple pieces of information to solve a terrorist -- a real terrorist threat. The first piece that comes in is from FAA 702. It says this guy is planning something, heads up, and everybody goes on alert.

The business record FISA says this guy is talking to a guy in New York City who has contacts with two other terrorist organizations, one and two out. So what you've done is you've used the FAA 702 to point to the guy in Colorado and the business record FISA to say, here's -- I shouldn't --

(Laughter)

GEN. ALEXANDER: -- here's how the network works. And so you see how both of those comes. But Customs and Border Patrol added some information in, and FBI agents added some information in. And what we're trying to do is give the agents enough information to stop the attack. And from my perspective, just that case alone, these paid for themselves, these paid for it. I think when you look at the type -- and the times that we've looked at that data, just the times and the numbers that we're looking at, it's reasonable and proportional.

And I turn it around and say, okay, so given that that's the best way we could come up with it, in the debate the question is, is there a better way to do it? Now, one of those is could we push the data to the providers? That's an option. Could we have more oversight?

You know, we have 12 to 1 already; maybe 14 to 1. But the reality is everybody who is looking at this doesn't say what we're doing is wrong; what they're doing is they're saying it's right. And then everybody who says it right, what they get is well, you're just rubberstamping it, find another guy.

So we had 14 and you guys all say it's right. Okay, what about you? You say it's right. Yeah. You're rubberstamping. You say it's right? You're rubberstamping. And so what we're going to do is everybody that says it's right is rubberstamping. And so my comment is we've got to step back and look at how we're going to defend the nation and protect civil liberties and privacy.

And you know, it can't be well, let's just stop doing it because we already know that doesn't work. We've got to have some program like this. And what I'm really asking for, Josh, is for you and others help us put those facts on the table. Let's have a discussion based on fact, not sensationalize and inflame the debate to such a point that everybody is racing over here and then finds out, oh, that's not true, and we have another terrorist attack because we stopped doing something that we needed. We can't do that.

MR. WILLIAMS: Let's take two more. Bart?

MR. GELLMAN: Hi, Bart Gellman. I like very much the idea of making this debate about the facts and I want to talk a little bit more about the oversight and see if I understand you correctly. I understand and stipulate that you collect examples internally of -- for example, inadvertent collection on Americans and you report those to Congress and the courts.

But you have -- in 702 you have a program that's authorized once a year. And the procedures are authorized, but you are not saying that the judges or Congress are examining any of the 45,000 selectors that you're using in that or what was the basis of the reasonable, articulable suspicion or you know, whether you use the right -- you made the right decision adequately supported to retain or not retain the communicators, I mean, they don't go into that, right?

GEN. ALEXANDER: They don't necessarily go into it, but our overseers do go into portions of that. Our general counsel, our IG, they do look at that and make sure that what we're doing is right. And what we do have to do is we look at this, and for example, let's say you make a mistake and there is somebody in the FATA who we thought was a bad guy, turns out to be a U.S. person, that's a violation.

We have to report that. We made a mistake, we thought Abu X was a bad guy, we made an assumption, all the indicators were there of a bad guy, here is how we came to that. We tell the court, we tell the administration, we tell Justice, we tell the IGs, we tell everybody in that chain, and then we say here is what we're going to do. And the court would normally say, okay, you have to expunge or purge that data.

And so we have a very good rule for working our way through this. And I think from my perspective it's done exceptionally well. And you're right, we do make mistakes, and we self-report those mistakes. And you know, one of the things that -- when the President first came onboard we had a huge set of mistakes and we were working through in 2009. And his comments, I can -- he said essentially I can see the values of these, but how do we ensure that we get these within compliance, we do everything exactly right. So we stood up our Directorate of Compliance.

And what they do is they systematically do what you're talking about. They go through and make sure that the way we've written these and the way that we're doing this is done exactly right. And we have a tremendous number of training programs that we send our people through so that when they look at this data they know exactly what they're doing. There are several courses, mandatory courses that everybody who touches this data has to go through. And they have to pass the test on those, it's not just go through the course, flick through it, and then say, okay, done, they have to pass the test and then they can use the data.

But they have to go through it just like that. So from my perspective, I think that's a great way to do it. Look at it this way. I think that's one of the best ways of providing oversight and compliance in the lawful intercept capability of any country in the world. Now, I'm not familiar with all the other countries in the world, but you have greater insights.

So you know, as you look at those, is there a better way to do it? Could we protect civil liberties and privacy better, and defend this nation better? That's what I think we need to do and you have some great insights on that, so we ought to put those on the table.

MR. WILLIAMS: Thank you all for your questions. General Alexander, thank you.

* * * * *