National Security Agency (NSA)

General Keith Alexander, Director of the NSA, Delivers Opening Keynote Remarks at the Billington Cybersecurity Summit

Speaker:
General Keith Alexander,
Director,
NSA

Location: National Press Club,
529 14th St NW,
Washington, DC 20045

Time: 8:10 a.m. EDT
Date: Wednesday, September 25, 2013

Transcript by
Federal News Service
Washington, D.C.

(Applause.) [Introduction by Thomas K. Billington, CEO, Billington CyberSecurity]

GEN KEITH ALEXANDER: I have a four-hour speech set up. Tom, thank you for that warm introduction, and thanks for the invitation here.

So I did have dental surgery. It's not that I started chewing tobacco, and I know Denny's wondering, what's going on? And Ed, it is good to see you here. Ed Tivol, an old friend – I use the "old" loosely – we worked together a long time ago – perhaps a little over 30 years ago for General Tom Weinstein, one of our mentors. And he set me out on this course. You know, I never wanted to stay in the military. I always thought, well, I'll get out after five years, and Tom Weinstein talked me into staying in. And he probably would have said, maybe you stayed six months too long.

And that's the part today – you know, the discussions that we have today is on cybersecurity. But I think, up front, I have to talk about media leaks. Not because I want to, not because I went in and had dental surgery to compare the discussion on media leaks to root canals and having your jaw lifted up, but if we're going to have a serious discussion on cybersecurity, we first have to address media leaks, and we have to get some of the facts out on the table. And I think the first thing that we have to have out on the table is, our mission is to defend this country, and our civil liberties and privacy. NSA and Cyber Command, that's our mission. And we can't do it without your help and without the tools our nation needs.

And so what I want to first do is talk to you about that. I think it's important that we put that on the table and that we get people to talk about the facts. Not to inflame it, not to sensationalize it, but to discuss those facts, because the future of this nation depends on our ability to protect us from terrorist attacks and cyber incidents. Those are the two things that can really impact this country, and they both significantly operate on that same network. So I want to step back. What I'm going to do is walk through some of that with you for about the next two and a half hours, and then I'm going to shift over to cybersecurity. But I do have an ask there, and that ask is up front. We need your help. We need to get these facts out. We need our nation to understand why we need these tools, and what those tools mean to civil liberty and privacy and what they mean to defending this country.

Everyone in this room can remember 9/11, the impact it had on our country. Almost 3,000 people killed by terrorist events in New York, Pennsylvania and here in Washington. We remember how those firemen tried to save lives, and they themselves were killed. And what I most remember, and what I think you in this room really remember is the military picking up that flag and saying, we'll take it, we'll defend this country. And they did. And I'm proud of that. I think it's, look at what Dave Petraeus, Stan McChrystal, Bill McRaven, Ray Odierno, Marty Dempsey – look at what our nation has given to protect this country. They went into Iraq, they went into Afghanistan and, you know, a lot of lives from our soldiers, sailors, airmen and Marines were lost.

And NSA, in 2005, Denny, – I see some of the folks here that are from NSA, we said, we can help. We will help. We will provide the intelligence our troops need to survive and win. And we put those folks forward. Over 6,000 NSA employees went into Iraq and Afghanistan.

Dave Petraeus, in some of his memoirs, said that turned Iraq around. It shifted it to our favor and put it at where it needed to be. Twenty-two cryptologists have lost their lives in Iraq and Afghanistan. They're the heroes, not the media leaker. They're the ones that picked that flag up from the folks in New York and did what our nation needed them to do.

But wait, they did more. It's almost like the Ginsu Knife – that's a joke. (Laughter.) They did more. We understand our job is to defend this country. It's a noble mission. I look at the folks that do this every day, and you say, these are great Americans. And what they've done is, they can see what the terrorists are trying to do coming into this country. And what we were blamed for as an intelligence community was not connecting the dots, because the FBI had one set of data, CIA, NSA and the other intelligence agencies another. And we were blamed for not connecting the dots.

So we said, we need the ability to connect the dots, and we came up with a couple of programs. Business Records FISA is the key one to connect the dots, and it's the one that is most talked about, so that's the one that we need to focus on here today. What is that all about? How do we connect the dots with this? What is it?

It's been sensationalized and inflamed in much of the reporting, that we're listening to Americans' phone calls and reading their emails. That's flat wrong. Under FISA, we would have to have an individualized warrant to do that, period. Our job is foreign intelligence. What we do need is the call detail records that we get in 215. We need those to connect the dots from what NSA can see overseas to get that to what the FBI can see here in the States.

Those call detail records include the to, the from, the duration and the date and time of the call. There is no content. There is no names, just the numbers. That's it. That's all we asked for. That's what the courts gave us. Judge Egan wrote a great, 29-page opinion on this. You ought to read that. What do we do with that? When NSA has insights that a terrorist is trying to do something inside this country, and we can come up with a reasonable, articulable suspicion that they're associated with al-Qai'da-related groups, we can then take that number, open up this lockbox that has all this data in it, and look into it.

In 2012, less than 300 numbers were looked at. That's it. That's what we need to connect the dots. And I will tell you, although I can't go into detail, it provides us the speed and agility in crises like the Boston Marathon and the threats this summer. And so what's hyped up in a lot of the reporting, is that we're listening to your phone calls, we're reading your emails. That's not true. You know, Edmund Burke has this great saying: "All that it takes for evil to triumph is for good men to do nothing." We can't do anything if we don't know the threat is there. We have to know about the threat. We have to connect the dots.

We live in a great country. We really do. We are blessed. We really are. In the last week over 950 people were killed in Kenya, Syria, Iraq, Yemen and Afghanistan by terrorists. One week. And we are discussing more esoteric things here. Why? Because we've stopped the terrorist attacks here. We've been fortunate. And it's not been luck. It's our military that's out forward, and it's the intelligence community that's back here. It's NSA, CIA, DIA and FBI working together with our military and our state and local law enforcement. They keep us safe.

They can't do it without tools. So we're going to have a debate in this country. Do we give up those tools? I'm concerned that we'll make the wrong decision because the facts aren't on the table. You have to help us get those facts out.

So one of those sets of facts is, well, what about those compliance incidents? What is a compliance incident, and what do you mean? I mean, what are you guys doing? It sounds to me like you're out of control. I get this a lot.

There are two sets of authorities that we operate under. Overseas, we call it Executive Order 12333. Over the last decade, we have had 12 willful violations in that area, where people normally sitting overseas, have used the cryptologic system inappropriately.

All 12 people were held accountable. Most of them opted to retire or resigned. Two were given Article 15s, reduced in grade and lost half a month's pay for two months.

You want to know the interesting part? Most of it was against foreign nationals, not against American people. But they did something wrong, and we held them accountable. We did the right thing.

And so it's interesting for our allies to understand that the SIGINT system that we have and that we share with our allies, if we make a mistake, whether it's against a U.S. person or a foreign person, we hold ourselves accountable, and we report it.

I'll tell you something else. NSA is the best technical agency in the world, bar none. Now, I know many of you are saying, but what about the leaker? Yeah. We trusted him, and he betrayed that trust. He was an IT administrator responsible for moving data to a common website, and he stole some of that data. We trusted him, and he betrayed that trust. That won't happen again. We'll fix that.

But that doesn't make him a hero, stealing our data, going to China, going to Russia and doing what he's done to this country, because I'll tell you, the people that learn from this, are the ones that will hurt this nation and will hurt our people. They will learn from this. And the tools that were so effective over the last past decade will not be as effective in the future.

There was also a report of 2,776 incidents. And so, if you – if you think about those, what does NSA do with those incidents, and why is that important, and why do we need to discuss that?

Well, we're a technical agency where the Internet and the networks that we operate on are always changing. And our job is to ensure that we comply with the law. And if we make a mistake, we self-report. We call those incidents or violations. Some people immediately jump that to privacy violations. That is wrong.

Of the 2,776 incidents in that report, 2,065 are roamers, or telephones that came into the United States that were not authorized to collect in the United States. The Department of Justice

and the courts don't call that a violation, but NSA tracks that, in an endeavor to always do better to get out in front of some of these.

That leaves 711 over a year. The majority of those are foreign. So of the 2,776, about 5 percent are on U.S. persons. And those are considered, like, typing in a number. If you – many of you now have hopefully passwords on your computer, and how often do you type in the wrong one and have to do it again? Every one of those would be a violation.

And here's the key for our privacy in this area. If we do make a mistake, we report it. Any data that is collected is purged, and we have to prove that to the court. We self-report to the DNI, to DOD, to the Department of Justice, to Congress, and to the courts, in every case. We don't step back. And some of these, if you've read, and you see from the courts' opinions, are ones that would make you say, wow, I'd really not like to have this one get out. But we will do the right thing in every case - and that's what we've done.

And what that means for you and the American people, is that you are guaranteed that we will do everything we can to protect your civil liberties, your privacy - and to defend this country. That's our job, and that's what we do.

You know, as I look out on all this, and I think about what's gone on over the last three-plus months, we've had a lot of discussion, but very little has been nested in those facts.

Congress is back in session. This is going to pick up. The American people have to weigh in and have to help us get the tools we need to defend this country and protect our civil liberties and privacy.

What I can tell you is that we're trying to be more transparent. It's hard for an agency that for the last 60 years has been invisible. And now we need to be transparent. And we're working to do that.

But I will tell you, when you look at what NSA has done for this country, has done with our armed forces… they are the noble people. They have earned your respect. They're the ones that, every weekend for the last eight years, the CT folks have been in, working for this country. Every weekend for eight years since I've been there. Think about that. Twenty-four hours a day, seven days a week, they're there to defend us. They need the tools to do it. You have to help us get there.

So those are my thoughts on the media leaks, not that I feel strongly about that. (Laughter.)

I would tell you another thing. I need to address two other portions of this, for many of you in industry. This is a compelled relationship, from the courts to industry to provide the data that we need. Industry isn't driving up the NSA dumping off U.S. persons' or foreign persons' data to us. What they're doing is they're providing what the courts have directed them to provide, which is, ironically, the same information that other countries demand of industry in a compelled lawful enforcement venue.

Our industry folks have taken a beating on this, and it's wrong. They're only doing what our nation has asked them, what other nations have needed from them, and what we have done together. We talked about 54 terrorist events that have been stopped - 13 in the United States, 41 overseas, 25 in Europe. It would not have been possible without that capability. And so industry has done what we've asked them to do. They've saved lives, here and abroad.

And our allies have benefited from that. Many people have asked me, how has this impacted your relationship with allies? Here's what I get: Keep working with us. The intelligence you get us to defend our country is what we really need. That's the fact. That's what I get. They say, we see a lot of stuff political out there. Please don't stop. We need your help. And you know what? We need their help too. And we have to have, and come up with a way of working together.

So in all of this, there's a couple things that I would put on the table. You know, I use that Edmund Burke comment about all that is necessary for the triumph is evil – of evil is for good men to do nothing. You know, a couple of things I'm really proud of. This country stood up on Syria. And that's the right thing to do. Fourteen hundred people were killed in a chemical attack, or more, and we stood up. And now there is discussions on getting rid of those. It would not have happened without this nation standing up.

And the partnership with our allies is also important, and we need to – and one of the things that the Director of National Intelligence and the White House and others have asked us to look at is options that we can put on the table of how we'll work with our allies in the future. And I think that's important.

So I had to start with the media leaks, if we were going to have a serious talk on cybersecurity. So let's shift to cybersecurity.

You know, when you look at what's going on, it's the same network, the same technical skills. And Debbie Plunkett will be up here after me, and she told me to just hype this a little. Is this helping, Debbie? (Laughter.)

You know, it is an honor and privilege to work with great people like Debbie, who runs Information Assurance Directorate for, what, the past five or six years – absolutely superb. They're the ones who, if you look back in our history in 1945, used and created SIGABA and SIGSALY, our encryption capabilities that were not broken by the enemy while we broke both ENIGMA and the RED and PURPLE codes. They do that today for our country. They do it for our government. And they do an absolutely superb job. And so thanks, Debbie, for what you and the entire Information Assurance workforce does every day. And I know your talk will pick up everything that I missed and answer every question that I failed to answer. Good luck with that. (Laughter.)

So cybersecurity. Same networks. Same technical skills. Same legal framework. A lot going on.

Two things that can hurt us: terrorism and cyber. And cyber is the easiest one to get at us.

Look at what's happened in the past year: over 300 distributed denial-of-service attacks on Wall Street. We saw destructive attacks in August of 2012 against Saudi Aramco and RasGas. We've seen destructive attacks against South Korea. What that says to me is this is going to pick up. It's going to get worse. And we have to get a number of things done to protect this country.

I want to talk about five different areas that NSA and Cyber Command are working together, that I think are important to our country. And the top priorities – I'm going to start out with a trained and ready force.

You know, the most important thing that we can do is train our people. The best in the world. That's what the American people expect of our military and of our intelligence community. And that's what we're doing. Why?

In this area, technical skills really matter. They really do. So we're engaged in a multiyear effort with the services to train our forces. And they've trained approximately one-third of the force in 2013. They'll do about one-third in 2014 and one-third in 2015. A huge step forward.

And the service chiefs have stood up and pushed those forces forward. Despite sequestration, despite all the battles that are going on in the Pentagon, they've stood up and they've all agreed, that this is a threat that we have to address as a military for the good of our nation.

We have teams that are fully operational now, that are working side by side with NSA to defend this country.

We've also activated a Cyber National Mission Force Headquarters. This is the one that would react to an attack on the country or attack on the Defense Department. And we will ensure that we have the best force anywhere in the world.

I'll tell you that we're also conducting exercises, such as Cyber Guard and Cyber Flag, that includes the combatant commands, the Guard and the Reserves, and interagency participation to develop the tactics, the techniques and procedures, and the working relationships needed for defending the nation in conducting operations in cyberspace.

Cyber Command provides cyber support elements to every combatant command today. We're refining our operational concepts and our command and control. And I think in doing that, that second part, coming up with the operational concepts and the command and control, is absolutely vital for the future. How does a force like this operate? How does NSA and Cyber Command work with FBI, with DHS? Great partnerships. And I'll just give a callout to both FBI, DHS, and I think NIST will be here later, Pat Gallagher, absolutely superb partners.

It takes a team to do this. Our job is to defend the nation. FBI is the one inside the country defending it, and DHS is setting the standards along with NIST.

One of the things that we have to fix, especially in the Defense Department – and I'm not sure, Debbie, if you're going to talk about this, but I'm going to enter into it, and hopefully I won't steal your thunder – we need a defensible architecture.

The legacy architecture that we have today has a number of problems with it. We have 15,000 enclaves. It is almost impossible to see what's going on in every one of those enclaves. Think of this as all of these tables in this room, and you want to know what somebody's writing in their notes, and they're 10 tables over. There is no way for you to know that. I mean, that's a good thing, probably. But there's no way to see attacks coming in. And if they get to one table, everybody else is open.

Our architecture needs to be redefined. And I think that cloud architecture that's been pushed forward for the joint information environment and the intel community's IT environment is where our nation needs to be, a thin, virtual, cloud environment. And it offers some great capabilities for the future.

First, in patching. Think about patching these tables. If we were to just pass cards around, and everybody started to patch, and you did what was said on the cards, how long it would take to distribute those cards amongst all these tables. Then think about 15,000 enclaves trying to patch their networks at network speed by a series of system administrators that work for each enclave. What is the probability that somebody will make a mistake? One. It's a hundred percent. Or that they will be too long? And the adversary will find that vulnerability and penetrate the system? So the way we're set up today is not where we need to be.

In the thin virtual cloud, you could essentially fix the entire network within a few minutes. You could push that out, do all the patching, all the vulnerability, scanning and everything you need in a few minutes. Could be done centrally, and you could remove the humans from the loop in that and put them where you need to be – where they need to be - in protecting the networks.

But there is other things that you can do in this as well. By having a thin virtual architecture, each system is a system that we see being scanned by an adversary; we can break that down and put it in a new place. You can jump networks, you can jump databases, and you can jump your actual own system and make it very difficult for adversaries to exploit.

So we need to go to that defensible architecture. I think that's the wave of the future and something that's vitally important for our country.

Shared situational awareness is another thing that we need to do, we need to address. What do I mean about shared situational awareness? You know, this is something that's interesting; if you were to ask somebody to describe the recent exploit or attack into your network, ask the IT people to draw you a picture. Hey, show me what that looks like, because I just want to understand what happened.

And so they'll talk about the domain control issue – you know, it's almost like a pilot; they start with the domain control and they show you this coming in, and then they say, OK, you know, it was like this and then this happened and they got in… and bad things, and we were had, and it's bad; it's going to take weeks, months, years to get them out.

How does it look? You know, let me ask you another – think about another thing. Right after that, say, well, how are we going to fix it? Draw me a picture of that with all these enclaves. If it's infected all the tables here, how are you going to systematically repair that and get the adversary out? It's a big problem. And if you can't see it and you can't get the humans to understand it, how do you get them all on the same sheet of music to accomplish those goals? That's very, very difficult.

And, if you widen it and say, so where's the adversary coming from, and how are they getting into this country? What's Cyber Command's role? What's NSA's role? And how do you see that? How do our allies see that, and how do we work together?

And the answer is nobody sees it. Today, we don't have the shared situational awareness that we need. And this is going to be a key capability for the future.

So we're developing a common operational picture. I think that is absolutely important for that nation and for our Defense Department, for Cyber Command, for NSA. We're sharing it with DHS, with FBI, with CIA, with all the combatant commands and with some of our allies. And I think it's a great way to go in the future.

I spent a lot of time on media leaks upfront, and I did that for a couple of reasons. And one of those, in cybersecurity, we need to work with industry. We absolutely need to work with industry. Industry owns and operate 85 to 90-plus percent of our networks.

So here is the issue that we have on the table. Who's responsible for defending the country from an attack, and who attacks back?

And, you know, one of the options that we could put on the table is we say, well, let industry do that. And let me just explain the problem that you get into as soon as you do that. That let's say bank one is being attacked, and they fire back from the point from where they think the attack is coming from, and they wipe out that capability. Oops. That was just a network the adversary was using in a neutral country, and they took it out. Sorry. But that's what they would see from their end. And what that would create is a problem in physical space where that country is now mad at us for doing something, and we have problems.

So what you quickly get to is, this is a responsibility of our government to defend the country from attacks like that and to respond back. And it's the president and the secretary, their responsibility to tell us when and what we should do. We provide the options.

But we have to work with industry because we can't see it. You know, this gets right back to that Edmund Burke comment. If we can't see it, we can't respond to it. And the attacks

on Wall Street, what we can do is tell you how they went down and how bad they were, but if we can't work with industry, if we can't share information with them, we won't be able to stop it. And we have to do that at network speed. We have to share what we know about those threats, and they have to tell us what they see. And this is where the Internet services providers are critical to this, not just here but with our allies and others. And we have to come together and figure out how we're going to do that. But I will tell you it takes industry. And so if you think about the problems with the media leaks and the issues that we have there, we have to resolve that because industry is critical to defending our country and cybersecurity, and the partnership is critical.

And Congress is working their way through. I'll tell you that, you know, the Senate Select Committee on Intelligence, shared by Senator Feinstein and Senator Chambliss, the co-chair, and the House Permanent Select Committee on Intelligence, chaired by Congressman Mike Rogers and vice chaired by Congressman Dutch Ruppersberger, are superb to work with, in both sides of this. They stood up on the media leaks when it wasn't popular to do it, and they're pushing for cyber legislation, and trying to resolve the things that industry thinks they need, and what our government needs, for us to work together. But we're going to have to do both. This is going to be critical for our country.

And so what I would say is we look at what's going on with media leaks and what's happened to industry as a consequence of that, we need to fix this. Industry has done the right thing. They're doing what our nation has asked them. And now we need industry to work us in cyber legislation.

And I think our allies are a key part of it. You know, these networks go all the way around the world. Most of the cables coming from the Atlantic come from the United Kingdom, about two-thirds of them. Makes pretty good sense that if the United Kingdom could clean that part, we protect this part, we have the basis of an alliance. France, Denmark and Spain are the other drops of those things coming from the Atlantic. And we ought to figure out how to partner with them in this area, and we're working that.

Finally, I want to talk about authorities. Under media leaks, I gave you a couple of issues that we need. We need the tools to protect this country. And in cybersecurity, we need authorities as well.

Necessary authorities do exist within our executive branch for most of this, and we have worked with our interagency partners to define clear roles and responsibilities, and that's between FBI, DHS, NSA and Cyber Command. And I think we have those clear lines.

But what we do need to do is we need to work with Congress on additional legislation regarding cybersecurity and our private industry. And that specifically is how we will share information and how we'll provide liability protection to them. Those are the key issues that have to come out of this.

We also have to clarify the rules of engagement. What is expected of us? This is a difficult topic. You know, we don't want NSA and Cyber Command doing something

irresponsible. On the other hand, we don't want NSA and Cyber Command waiting for the authorities while Wall Street is taken down in cyber. So we have a dilemma. How do we work that? And I'll tell you that the folks at U.S. Cyber Command, with NSA, are working within the Defense Department and the interagency to look at the authorities that we need and how we'll actually do this.

And it very closely follows what you would expect us to do as if this were a missile attack on our country. How do we go through those authorities? How do we set up the conference calls? How do we go to the Secretary of Defense and the president and get the authorities that we need and give them the options. And we're working our way through that. And I think the government has done a great job moving that forward. There's going to be more that we need, and that's the legislation.

You know, I think – to sum up on the cybersecurity side, no single public or private entity has all the required knowledge, resources, authorities, or capabilities. We have to work together. And I think we have to do that between government and industry, and with our allies. And we have to address these issues as a team. So I want to – I'm going to stop. I know the clock is counting down here. I want to just address a couple things to summarize where we are when we talk about a team.

This is a great country that we have. It really is. Look at – you know, I have 15 grandchildren. And we were talking about that with Bill and the folks here. You know, and one of – the one-year old got an iPad, one year – she was almost two, but to show you that girls are getting faster than the boys here. She grabbed one of the iPads. She could grab that iPad go to a Netflix thing and pull up the cartoon. And she can't hardly talk, but she can do that on the iPad. It's amazing.

Look at where these children will be in the future and the capabilities. Look at what industry has done in this area. It is absolutely superb. It would not have been possible if we didn't have the military and the intelligence community protecting this nation. Nine hundred and fifty people were killed over the last week - and look at our country and look at what we enjoy. And it's not by accident. It's by a lot of hard work of people behind the scenes, that are doing what our nation expects them to do. They do it because it's the right thing. They do it as part of a team.

That military and intelligence team that defends this country, it is the greatest honor and privilege I have ever had to serve with them, because they're doing what the country needs them to do. It is phenomenal to see some of these young folks come in, know they have stopped a terrorist attack, and they can't tell anybody, other than us. And you know what they say? That's good enough. We save lives and people over there will never know that they were at risk. We got to partner with the FBI, the greatest law enforcement agency in the world, and they stopped something. And the American people will never know how bad it could have been.

Think about what happened in 2009, the New York City subway. Both of those authorities were used to help stop that. Those people are now in prison. Team America did it. Great partnership, just what you would expect. Now, here's the deal. We need tools to do that,

both in the media side, in our counterterrorism and in our cyber security. We can't do that without your help. That's what our nation needs. That's my ask of you. You are the American people.

You know, the – there's a lot of people out there screaming and yelling. We're not listening to their phone calls, we're not reading their email. We're defending this country. We'll do it right. We'll hold ourselves accountable. We'll report every incident. But we need tools to protect this nation. If you take those away, think about the last week and what will happen in the future. My concern is, if you think it's bad now, we get several of those things that happened in Nairobi in this country and we have a whole different ballgame. And we will have failed.

The only thing for evil to triumph is for good men to do nothing. And good men can't act without intelligence. We need that information and we need your help in doing it. So with that, let me open it up to questions. Somebody just say, what are those? Those are interrogatives posed to gain information. (Laughter.)

MODERATOR: Thank you very, sir. If I could please ask you to address your questions on notecards and please raise your hand. We will pick up the notecards. And please, please do address them. And I just would like to make a quick announcement before the – as the questions arise, if I might, sir.

Just want to thank those who made today's event possible: the lunch sponsor, Northrop Grumman, our diamond sponsors, RSA, Raytheon, Guidance Software, Hewlett Packard, General Dynamics, JonesNCTI and Kaspersky Lab, our exhibitors, Information Security Solutions, NetIQ, AirPatrol and IEEE. And we also have our media sponsors: Homeland Security Today, CSFI and Set Aside Alert. And thank you for allowing me that opportunity to thank those who made today's event possible.

Questions – please do raise your hands and I would welcome them. Do you have one here?

GEN ALEXANDER: So before we get to questions, you might have thought I was a little emotional on the media leaks parts. Actually, I went in for dental surgery, and it's just the pain. (Laughter.) No, I really did have the dental surgery, but I do feel strongly about this country and what we ought to be doing for it.

MODERATOR: And it's very clear you do. And thank you for all you're doing to secure our country. We're honored.

First question regards the area of spear phishing. Spear phishing poses a pernicious threat. And with Cybersecurity Awareness starting in a week, what advice would you give C-level executives in the room to mitigate the spear phishing threat?

GEN ALEXANDER: What's pernicious? No, I'm just kidding. (Laughter.) I thought, I'd keep those pernishions out of here (laughs). Well, spear phishing, you know, most of this is somebody's got your credentials, right? You've got to come up with a way of defending on the

perimeter, understand how the spear phishing is going to get in. This is where they've put something in an email and they send it to you. If you get an email, and you click on the attachment, and it's saying, hey, I've got a million dollars for you, and you click on it, there ought to be something that jumps up on your screen that says you're an idiot for doing that. (Laughter.)

Now, here's what – you know, just to show you the sense of humor our folks have, they do that on mine. Every time I click on that, they have – they stop it and just put on there, you're an idiot, don't do that. But you'd be surprised at how often that works. Now, the interesting part is it's not always, hey, I've got a million dollars; would you just reach out and I'll help and I'll share it with you? Oftentimes it will be things like medical care, a change in the medical care program for your agency or your company. And they send it and it looks very real because they've done the research.

So you do have to be careful of what you click on, because once that happens the payload, or the capability that the adversary has created, is dropped down on your system. And once that happens, they're in. So you've got to have a way of protecting your system. Part of that is by setting up in your defenses, not letting attachments through or sterilizing those attachments. And many of the antivirus communities already do that and they provide great capability.

Next question. No more? Oh good. (Laughs.) Look at the time.

MODERATOR: We have a question on where – the small business community. For those small businesses that represent the innovation and – much of the innovation and the growth in our economy, but those companies often don't have the resources of a large company. What would you suggest to small businesses, particularly in our CSPAN audience, who might be listening today?

GEN ALEXANDER: Well, that's a great question. You know – you know I can remember this with Bill Aikens. You know, I gave him this set of cards – he was one of my bosses once. And he would always grab the notecards and say, I don't need to read them ahead of time, I'll just read them up on the stage. So I gave him the first two pages. In the third page I wrote out: You are on your own.

So he reads the first two pages and he gets to that third one. It goes, you're on your own. He looks up and he goes, now what? Well, for small businesses, you're not on your own. I think there are some great capabilities. In fact, I know Debbie's going to hit on part of this. So one of the great things that these agencies and other governments working together, with the Information Assurance Directorate, has come up with the SANS Institute on the top 20 things that you should do to protect your networks.

And these – and I think it's under 4.1 – version 4.1, is that right? Version 4.1 of the SANS Institute has the top 20 things that you should do to protect your network. If you do that, your network is going to be pretty darn secure. It's going to be tough for somebody to get

through. So if you're a small business, that's all publicly available information. I would just reach out and get that.

If your IT people – your information technology people don't understand it, they can reach out to players. There are great folks at SANS Institute. There's great folks at DHS and at NSA's Information Assurance. We have a public website on that. You can grab that from that website. It's all free, and it's great advice. Just follow that. In fact, if you do the top five you hit most of the key issues that we have.

And I don't know – are you going to cover some of that, Debbie?

DEBORA PLUNKETT: I am now. (Laughter.)

DEN ALEXANDER: Oh, look at the time, huh?

MODERATOR: Thank you. Question regards the information sharing area. Let me grab that. What is the – regarding information sharing – what rules of engagement do you find are necessary in that?

GEN ALEXANDER: Well, let me – let me talk about information sharing, and I'll expand on your question a little bit. What do we need to do between government and industry to share our information and what's the kind of information that we're talking about sharing? We're not talking about sharing our privacy information. We're talking about sharing vulnerabilities and threat information. So it has nothing to do with civil liberties and privacy, and everything to do with protecting our systems.

So think about the great companies like McAfee, Symantec, Mandiant and others that have all these antivirus capabilities, all this malware that they've detected. Well, the government has some too. We have a few good people, more than a few, that have good technical skills, that know classified information, about what our adversaries could do to this country. How do we share that classified information with industry?

So here's my thought, here's our thoughts on that. If you look at the networks of this nation, they ride over the Internet, and the Internet service providers are the ones that provide the basic help for this country. So they're the key point of defense. AT&T, Verizon, Sprint, L3, CenturyLink – those are the companies that own and operate the underlying networks of this nation. So how do we share with them and they help protect? What's the relationship there? And the answer is we've got to share it with them, and other companies, and potentially other countries and provide that information that says, when I see this, I'm going to tell NSA, Cyber Command, DHS and FBI, we got a problem, and do it at network speed, so they can react. They can also call out and say, we need help here, or I see this new interesting thing, piece of malware over here, and share that.

In the information-sharing environment, we need the authority for them to share with us and for us to share with them. Our parts oftentimes could be classified, so we need the way of protecting it. And when we give them something to protect the networks, and we make a

mistake, they shouldn't be held liable for it, so we need the liability protection. So we need that way of information sharing for the country.

Next question?

MODERATOR: We have two questions regarding the cloud. The first one is how do you balance the advantages of centralized architectures such as cloud computing with the risk of having all of your security eggs, as this questioner says, in one basket?

GEN ALEXANDER: That's a great question. And there's a couple of issues that we need to put out here on the cloud versus the legacy architecture. There is an assumption that having all your stuff diversified in 15,000 enclaves is more defensible, but that's just the opposite. In this case, I'm not talking about putting everything in one bank. The cloud is in itself a distributed architecture that we would expect.

Now, there are some things that we need for this country to defend ourselves in cyber, to defend you in cyber. Everybody in this room has either an iPhone, and Android, or some mobile device on them today. What does that communicate with, and how do we protect it? Think about that. That's step one. Where's the cloud in this? And what can we do in the cloud that ensures the protection of mobile environment and the cloud environment?

There are things that we can do in the cloud that we can't in our legacy architecture. Specifically, we can encrypt data sets. We can come up with ways of acknowledging who you are, having a secure set of encryption that far exceeds where we are today. We can identify when actors are trying to steal data in real time. Media leaks would have been stopped by that capability. These are great attributes, and you can encrypt it, so when somebody steals it, all they get is encrypted ones and zeros.

This is a great thing forward where we need to go, and there is going to be a lot that's going to go on in this area. I think it's the future, and it's something that we have to embrace and figure out how we match that cloud environment with the mobile environment, because that's where we're all going to be operating. And I think what's coming out of there is exciting and good for our country. And it's part of that future architecture that the Defense Department and the intel community are doing.

And I would tell you one of the thing's NSA has developed: a secure cloud called Accumulo. I'm not selling it; it's free. It's free. You go out there and get it yourself. It's openware. And it's got a security layer and a real-time tipping and queuing capability, and it's free.

MODERATOR: Thank you very much. I know you're under a tight schedule, so I'll limit it to two more questions. The first regards what specific actions can and will meet – will most likely be taken to avoid future media leaks. I know you've mentioned that, might elaborate, the systems administrators, and particularly the two-person rule and the obstacle that might be posed by removable media. So if you could just take a shot at that question.

GEN ALEXANDER: Well, there's a number of things, and you hit a couple of those right there. First, removable media, two-person rule on this – you know, system administrators need removable media to boot systems and stuff, so we have to now put in a two-person, and have implemented a two-person rule even for system administrators.

But there's more that goes on here. When you red-team it, you'd say, well, if you fix the removable media, all they need to do is go into the server room and take a disk, so you need to put a two-person rule on the server rooms. We've done that. There's a lot that's going to have to be done because one person has betrayed our trust and confidence. That's the right thing to do. Let's go fix that. Our technology Directorate, Lonny Anderson and the group, have done a phenomenal job laying out a whole series of things that they've done in the past 90 days to secure our network. And we shared that across the intelligence community, the Defense Department and with other agencies, and I think those are steps of the future.

And they've created some new tools to watch what people do on the network, to ensure that nobody does what this leaker did again. And I think that's great work, and again, that's all going to be shared with our partners out there.

MODERATOR: Thank you. The last question regards our critical infrastructure. To protect our country's most critical infrastructure from destructive cyberattacks, what authority do you feel USCYBERCOM, the NSA or – and/or the private sector needs that they might not have now?

GEN ALEXANDER: Well, I think that the most important thing that we need is we need the ability to share information with industry. Right now we can't see what's hitting industry. We have no real-time tipping and queuing capability between industry and the government. And I don't say that that has to come uniquely to Cyber Command and NSA. I agree that if we do this in a transparent process, send it to the government all at once, DHS, FBI, NSA and Cyber Command, that way everybody will know we're doing the right thing, it's transparent, and we get that information at network speed. FBI can look at to see if it's law enforcement, criminal-related, NSA can look at it to see if there's a foreign nexus, and Cyber Command can look at it and say, what do I have to do to defend the country given this information.

But you have to know the information. And right now what happens is the attack goes on, and we're brought in after the fact. I can guarantee you 100 percent of the time we cannot stop an attack after the fact. (Laughter.) Those are quotable quotes. (Laughter.) Okay, so after, all we're going to do is forensics. We can come in and say, it was really bad. And you can agree with us and say, yeah, it was really bad, and you're probably going to have to redo your whole network; yep, it's going to be a long time; yep, it's going to cost a lot of money; wish we had something up front to stop this, maybe information sharing. So that legislation that we're pushing for is absolutely important for our country.

So just to summarize, if I could, thanks for taking the time to listen. There's the one ask I have of all of you, and that's help us get the tools that we need to defend this country and protect our civil liberties and privacy. We'll do our part. We'll hold ourselves accountable. We'll protect civil liberties and privacy, and we'll defend this nation, and we will do it right.

Thank you, folks. (Applause.)

MODERATOR: General, we were honored that you joined us today, and thank you very much for all you're doing to secure our country. And I think the standing ovation speaks for itself. So thank you again, sir.

GEN ALEXANDER: Thank you.

(END)